機密情報交換サービス “パッケージプラス(R)トランスポーター”

鈴木　剛＊
渡邉優介＊

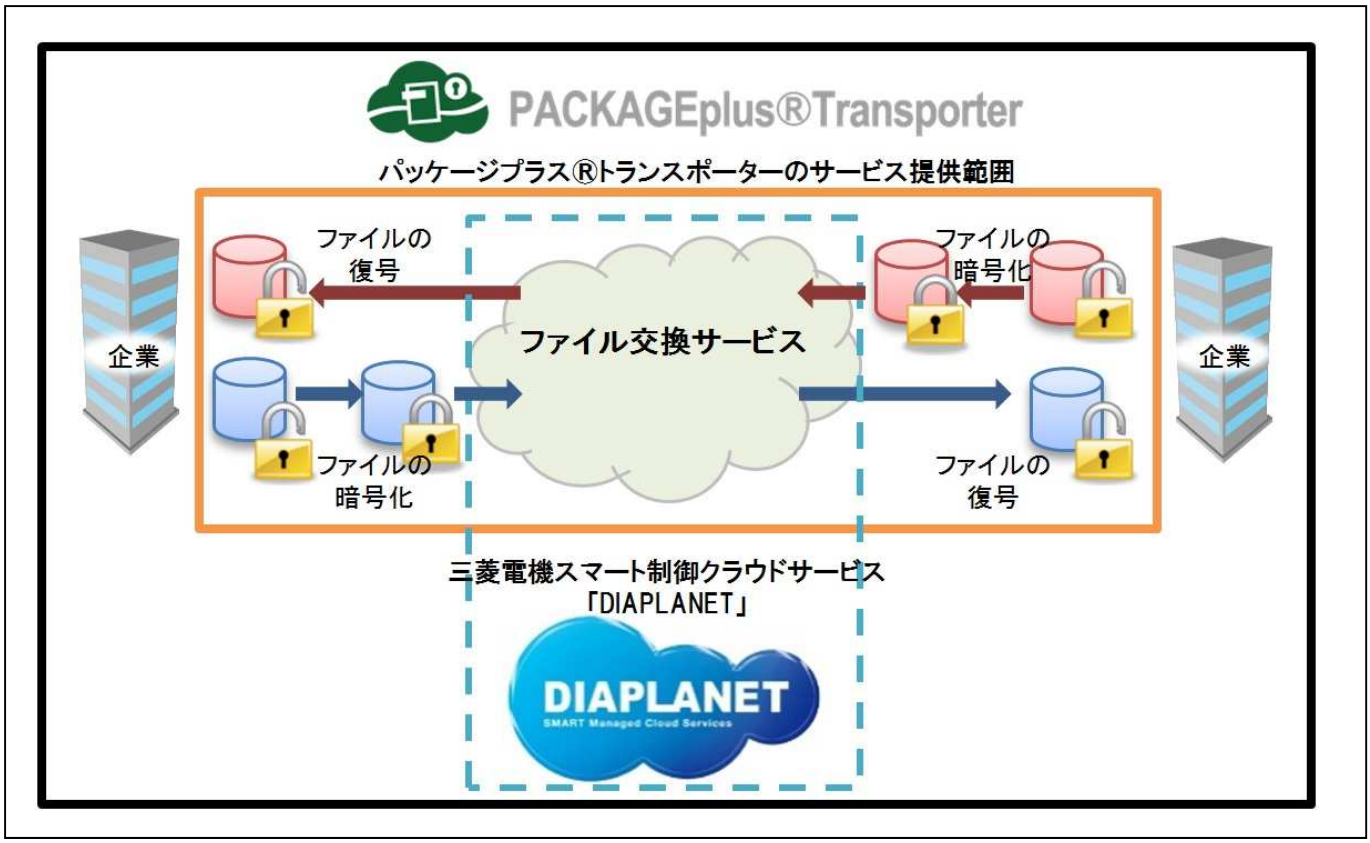
Confidential information exchange service “PACKAGEplus(R)Transporter”

要　旨

株式会社三菱電機ビジネスシステム(ＭＢ)では，企業間における機密情報ファイル交換を，三菱電機の”関数型暗号”[(1)]が実装された三菱電機スマート制御クラウドサービス“DIAPLANET”[(2)]上で実現する，機密情報のファイル交換サービス”パッケージプラス トランスポーター”の提供を 2016 年 1 月より開始した。

機密情報や個人情報の漏えい・改ざんは，ひとたび発生すると企業経営の根本を揺るがしかねない深刻な社会的な問題へと発展するケースが少なくない。一方で，従来紙や電子メディアで行われてきた企業間のデータ受け渡し業務は，ネットワークを介したファイル交換サービスの利用が急速に高まりつつある。

ＭＢでは，このような市場のニーズに応えるべく，機密情報のファイル交換サービス”パッケージプラス トランスポーター”によるファイル交換サービスを，高セキュリティ・高信頼技術の強みを活かした“DIAPLANET”を使用して提供することで，企業間での機密情報の安心・安全なファイル交換を実現している。



パッケージプラス トランスポーターのサービス提供範囲

機密情報交換サービス”パッケージプラス トランスポーター”は，企業と企業が行うファイル交換を，三菱電機スマート制御クラウドサービス”DIAPLANET”を使用して提供している。これにより，安心・安全な電子データ交換を実現している。

1．ま　え　が　き

企業間のデータの受け渡しは，紛失・盗難のリスク回避のため，インターネット等のネットワークを介したファイル交換サービス等の利用が急速に高まりつつあるが，インターネットの安全性に対する懸念は解消されていない。

機密情報や個人情報の漏えい・改ざんは，ひとたび発生すると企業経営の根本を揺るがしかねない深刻な社会的な問題へと発展するケースが少なくない。加えて，2016 年 1 月より運用の始まった”マイナンバー”(注1)を含んだ特定個人情報の受け渡しは，より安全な手段で行わなくてはならない。

ＭＢでは，このような市場のニーズに応えるべく，企業間で機密情報のファイル交換を安心・安全に実現するため，高セキュリティ・高信頼技術の強みを活かした“DIAPLANET”上でファイル交換を実行するサービス”パッケージプラストランスポーター”（以下，”本サービス”という。）の提供を開始した。

本稿では，本サービスの機能・特徴，および他社サービスにない特長について述べる。

2．本サービスの概要

本サービスは，企業間等の機密情報のファイル交換を安心・安全に実現するサービスである。

本サービスでは，ファイル交換相手を設定する機能により，指定した相手のみが復号できるという堅牢なセキュリティを維持したファイル交換を実現している。

さらに，本サービスにおけるファイル交換では，クライアント側の“Windows”(注2)アプリケーションで暗号化/復号の処理を行い，暗号化通信 HTTPS（Hypertext Transfer Protocol Secure） を組み合せることで，機密情報をより強固に保護する仕組みを採用した(図１)。

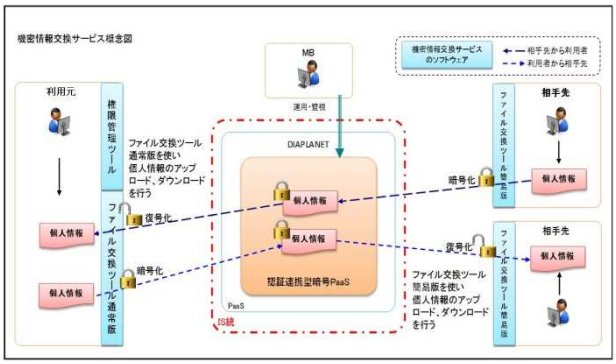


図１．機密情報交換サービスの概念図

（注１）マイナンバーは、内閣府大臣官房会計課長の登録商標です。

（注２）Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

3．本サービスの機能概要

三菱電機スマート制御クラウドサービス”DIAPLANET”は，これまでの大規模システム対応で培った高いレベルのセキュリティと信頼性により，安全・安心な運用環境を”PaaS（Platform as a Service）および SaaS（Software as a Service）”で提供する。

本サービスでは，”DIAPLANET”の提供する”認証認可機能”と”暗号 PaaS 機能”を利用している。本章では，本サービスが持っている，安全にファイル交換を行うための機能について紹介する（図２）。

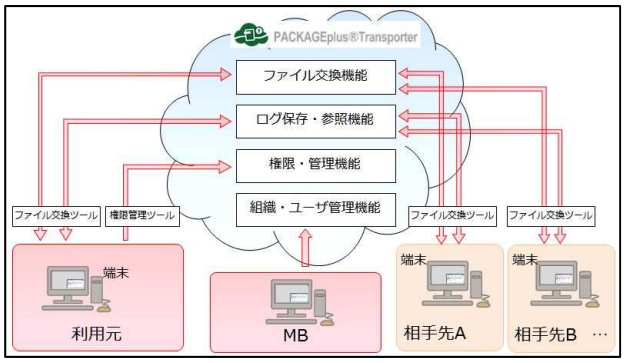


図２．機密情報交換サービスの機能図

3.1　本サービスを構成するツールと機能

本サービスは，機密情報の電子データを交換するための”ファイル交換ツール（通常版・簡易版）”と，利用元・相手先の情報等を設定する”権限管理ツール”，及びクラウド上で提供するサービスから構成される。各ツールが提供する機能は表１の通りである。

表１．機密情報交換サービスの機能

	ファイル交換ツール通常版	ファイル交換ツール簡易版	権限管理ツール
使用者	利用元、相手先	相手先	利用元(管理者)
機能	ファイルアップロード		ファイル交換相手設定
	ファイルダウンロード		利用者名変更
	ファイル削除		相手先名変更
	ファイル暗号化・復号※1		ファイル領域の初期化
	ファイル交換ログ参照		パスワードリセット
	ダウンロード通知		変更ログ参照
	自動ダウンロード		
	パスワード変更		
	複数の相手とファイル交換	×	
	フォルダー管理	×	

※1 三菱電機の関数型暗号を使用

3.2　”利用元”と”相手先”の概念

一般のファイル交換サービスでは，送信者と受信者の間で一対一でのファイルの授受を行うが，本サービスでは，図３に示すように同時に複数の相手先とファイル

の授受が行える。また，管理者側（利用元）では，複数の社員等（担当者）が利用できるように，担当者別に複数の ID（identifier：識別子）を保有できる。

これらの設定は，後述する権限管理ツールで行い，設定された情報はクラウド上の本サービスの領域内に管理データとして保存される。

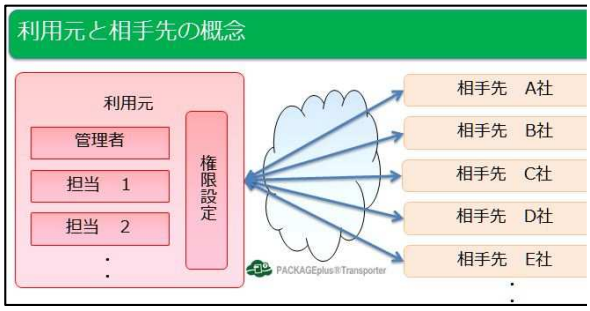


図３．利用元と相手先の概念

利用元：本サービスを契約した企業や部門。
複数の企業や部門等とファイル（データ）交換を行い，複数の相手先の管理ができる。また，複数の担当者等がファイル交換を行なうことができる。

相手先：利用元がファイル交換を行う相手となる企業や部門。利用元のみとファイル交換を行うことができる。

3.3　ファイル交換ツール

機密情報を安全にファイル交換するためのクライアントツールである。利用用途によって，複数の相手先とファイルの交換を行う利用元が使用する通常版と，相手先が使用する簡易版を用意している。

利用できるファイル形式に制約はなく，パソコン等で使用できるファイルであればよい。機密情報のデータファイルだけでなく，プログラムファイル等の授受にも利用できる。

図４にファイル交換ツール利用の概念図を示す。

ファイルを相手方に送信する場合には，ファイル交換ツールを使用してファイルをクラウド上の本サービスにアップロードを行う。相手方から送信されたファイルを受信する場合は，ファイル交換ツールを使用してファイルのダウンロードを行う。

それぞれの端末で行った作業のログは本サービス上に保存され，それぞれの端末からのみ参照できる。

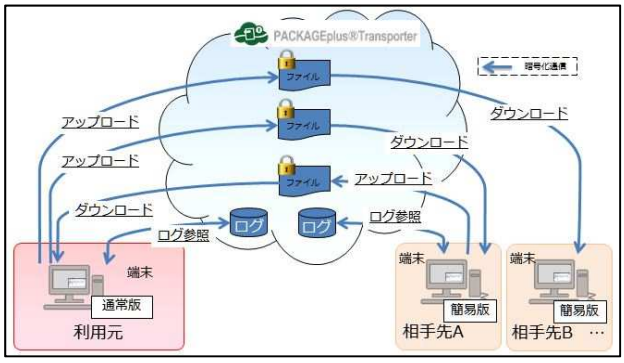


図４．ファイル交換ツールの概念図

なお，簡易版は，ファイルの送受信先が一つの場合だけに使用できるように設定されており，操作が簡単に行え，誤送信を防止している。それ以外の機能は通常版と同一である。

3.3.1　ファイル交換ツールの機能

利用元で使用する場合，ファイル交換ツールでは権限管理ツールで設定された，ファイル交換可能な全ての相手先を相手先セレクターで一覧することができ（図５①），さらに相手先毎のファイルのアップロード（送信）及びダウンロード（受信）の状況が確認できる。

また，アップロード（送信）したファイルを相手先がダウンロード（受信）し保存したかどうかの状況も把握することができる（図５②）。

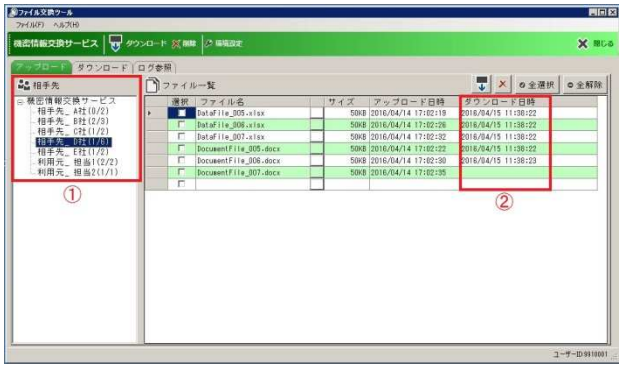


図５．ファイル交換ツールの”アップロード画面”例

一方，ダウンロード画面では，相手先が送ってきたファイルの一覧が，相手先毎に表示される（図６）。

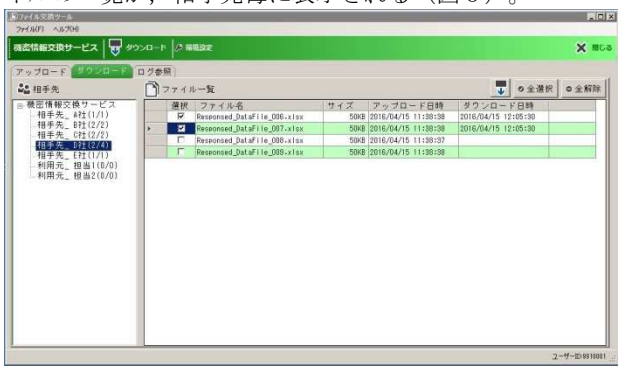


図６．ファイル交換ツールの”ダウンロード画面”例

送信元あるいは相手先が送ってきたファイルは，サーバ又はクライアント端末のローカルディスクのいずれかを選

択して保存するが，”環境設定”画面でのパラメータ設定によって，送信元あるいは相手先からの送信ファイルを自動的にサーバやクライアント端末のローカルディスクに保存することもできる（図７）。

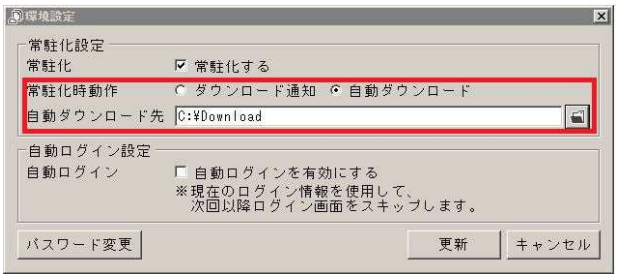


図７．環境設定画面での設定例

3.3.2　操作ログの記録・参照機能

ファイル交換ツールや権限管理ツールを操作した内容はログとして記録され，いつでも参照することができる（図８）。

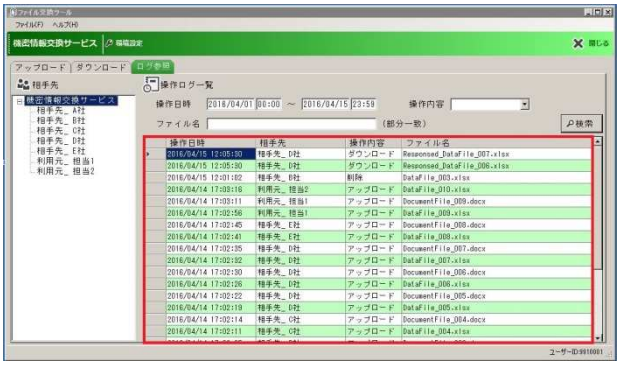


図８．操作ログ参照画面例

3.4　権限管理ツール

“権限管理ツール”は利用元で使用するツールであり，相手先の名称や，利用元の名称，利用元の社員等がファイル交換できる相手先を設定することができる（図９，図１０）。

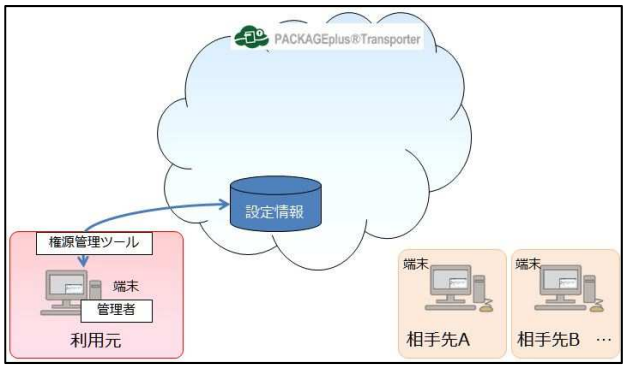


図９．権限管理ツールの概要

また，“権限管理ツール”は，相手先からの要請等によりパスワードをリセットする機能や，利用する相手先が変更になった場合等にファイルの交換領域を初期化する機能を備えている。

なお，利用元が設定した利用権限等の設定情報も，契約情報と同じようにクラウド上に保存される。

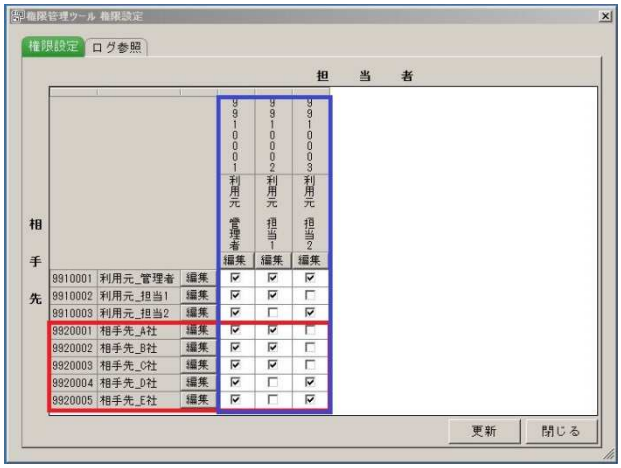


図１０．権限管理ツールの設定例

3.5　組織・ユーザーの管理

本サービスを利用する組織，ユーザーの情報は，ＭＢが契約情報を基に登録し，クラウド上に安全に保管される（図１１）。

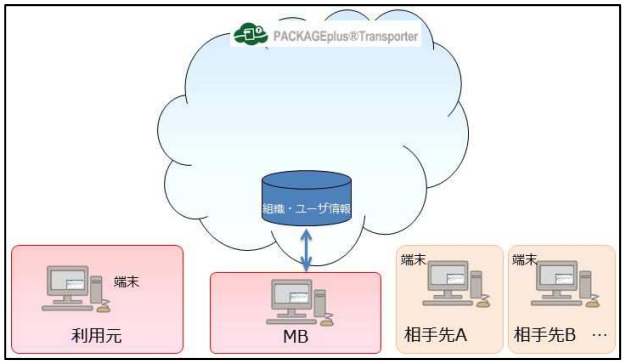


図１１．組織・ユーザー情報の管理

3.6　他社サービスにない特長

(1)機密性・完全性の確保

本サービスも他社のファイル交換サービスも，暗号化通信により通信経路を暗号化しファイルの送受信を行っているが，万一暗号化通信に脆弱性が発覚し（ 例：POODLE（Padding Oracle On Downgraded Legacy Encryption）：2014 年，SSL（Secure Sockets Layer）通信の脆弱性）ファイルが搾取されても，本サービスの場合はファイル自体に関数型暗号が施されているため情報漏えいや改ざんを防ぐことができる。

また，他社のファイル交換サービスはクラウド上で暗号化・復号が行われるが，本サービスでは利用元で暗号化されたファイルは，指定した相手先が受信するまで復号されないため，ファイルの機密性・完全性を保つことができる（図１２）。

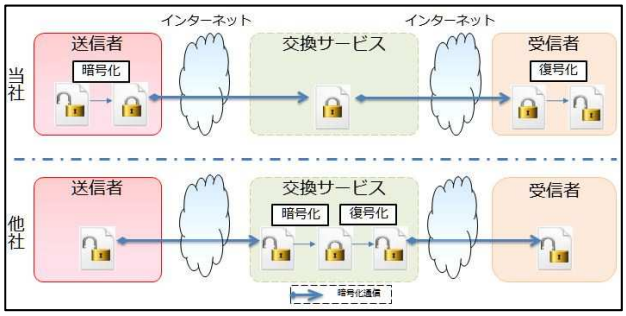


図１２．他社のファイル交換サービスとの比較（機密性・完全性の確保）

(2) 個人情報を必要としない

本サービスでは，設定情報に個人情報が無くても利用できることを大きな特長にしており，氏名・メールアドレス等の個人情報は一切必要としていない。

他社のサービスのように，自分宛てファイルが送信された場合，メールでの通知があると便利ではあるが，本サービスでは，クライアントツールのバックグラウンドでの常駐化機能（タスクトレイ）を備えることで，自分宛てのファイルが送信された場合に，自動ダウンロードできる仕組み及びバルーンメッセージによる通知を表示する仕組みとしている。

3.7　提供サービスの要件

本サービスが提供するサービスの要件は表２の通りである。

表２．提供サービスの要件

要件	内容
ファイル形式	制限なし
使用容量制限	5GB/契約企業
ファイル保持期間 ダウンロード済みファイル	24時間 初回ダウンロードから24時間経過後に自動削除
ファイル保持期間 未ダウンロードファイル	30日間 初回アップロードから30日経過後に自動削除
利用者によるユーザーID変更	不可能 サービス内で一意になる必要があるためMB管理
管理者による操作ログの一元管理	不可能 操作ログ表示はログイン中ユーザーの操作に限定
管理者によるダウンロードファイル保存先の一元管理	不可能 ダウンロードファイルは操作毎にユーザーが指定

４．関数型暗号とは

“関数型暗号”とは，三菱電機（株）が開発した安全性と利便性を両立できる暗号化の仕組みであり，従来の暗号化技術をさらに発展させた次世代の暗号化技術としてクラウド時代に求められる高度なセキュリティを実現している。

従来の暗号化技術とは異なり，“関数型暗号”では，アクセス権限の機能を取り入れており，データ提供者が指定した属性を持つ社員の秘密鍵でのみデータの復号を可能としているのが大きな特長である（図１３）。暗号化する場合に，例えば，そのデータの受信を許可する組織上の所属や役職をアクセス権限で定義しておくことによって，仮に復号のための鍵を持っていたとしても，人事異動等で該当の所属や役職等を離れた社員がデータを復号することができなくなるという仕組みになっている。

図１３の例では，復号できる条件を“営業部の課長，または部長（（営業部　and　課長）　or　部長）“としているため，開発部の課長やシステム管理者は復号できない。

また，人事異動等により所属部門や職位が変更になり，条件を満たさなくなった場合も復号できない。

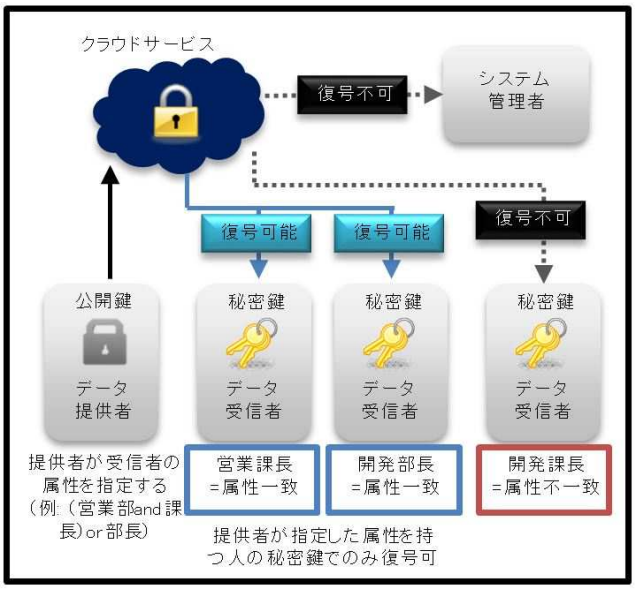


図１３．関数型暗号の概念図

上記のように組織情報など関数型暗号を組み合わせると細かいアクセス権限を設定できるが，アクセス権限を強化するためパブリックな共有クラウドサービスに組織情報を持ち込むと管理が煩雑になるという課題がある。そこで，本サービスでは，利用元から相手先にデータ送信する場合は個人名宛てに秘密鍵を送付するが，その逆に相手先から利用元にデータ送信する場合は，個人名宛てではなく利用元の職名宛てにファイルを送付する仕組みにして，職務上，アクセスが許可された属性を持つ社員だけがデータを復号できるようにしている。なお、復号に使用する属性を，複雑な組織情報ではなく，一部の役割に限定することによって，“関数型暗号”の特長を活かしつつ簡便に使用できるように考慮している。

５．む　す　び

今後もデータ交換の利用頻度は高くなることが予想され，より安全なデータ交換等を行なうための対策が必要となる。

ＭＢでは，今後増加する電子申請・申告（e-Gov[注３]，“eLTAX”[注４]）等のデータ交換をより簡単に，より安全に利用できる仕組みを”パッケージプラス”製品ラインナップとして揃え，安心・安全なデータ交換サービスをサポートするソフトを提供していく（図１４）。

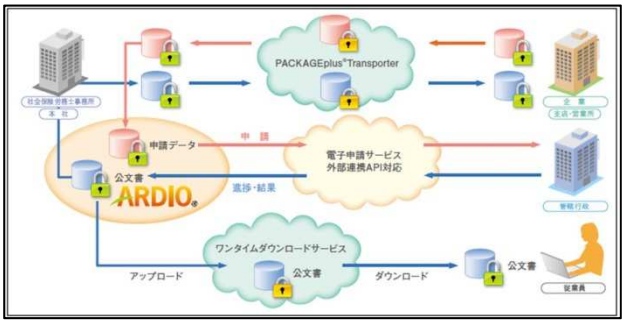


図１４．パッケージプラスの機能全体図

参考文献

（１）情報技術総合研究所：注目の研究・技術，関数型暗号，三菱電機（株）オフィシャルサイト
http://www.mitsubishielectric.co.jp/corporate/randd/spotlight/spotlight15.html

（２）トピックス，情報，スマート制御クラウドサービス”DIAPLANET”，三菱電機技報，90，No.1，19（2016.1）
http://www.mitsubishielectric.co.jp/corporate/giho/1601/pdf/1601007.pdf

---

（注 3）e-Gov：・電子政府の総合窓口（イーガブ）は,総務省行政管理局が運営する総合的な行政情報ポータルサイトです。

（注 4）eLTAX：エルタックス・地方税ポータルシステムの呼称で，一般社団法人地方税電子化協議会が開発・運用主体とする地方税の手続きを電子的に行うシステムです。

eLTAX は、一般社団法人地方税電子化協議会の登録商標です。