特集論文

機密情報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”

鈴木　剛*
渡邉優介*

Confidential Information File Exchange Service "PACKAGEplus Transporter"

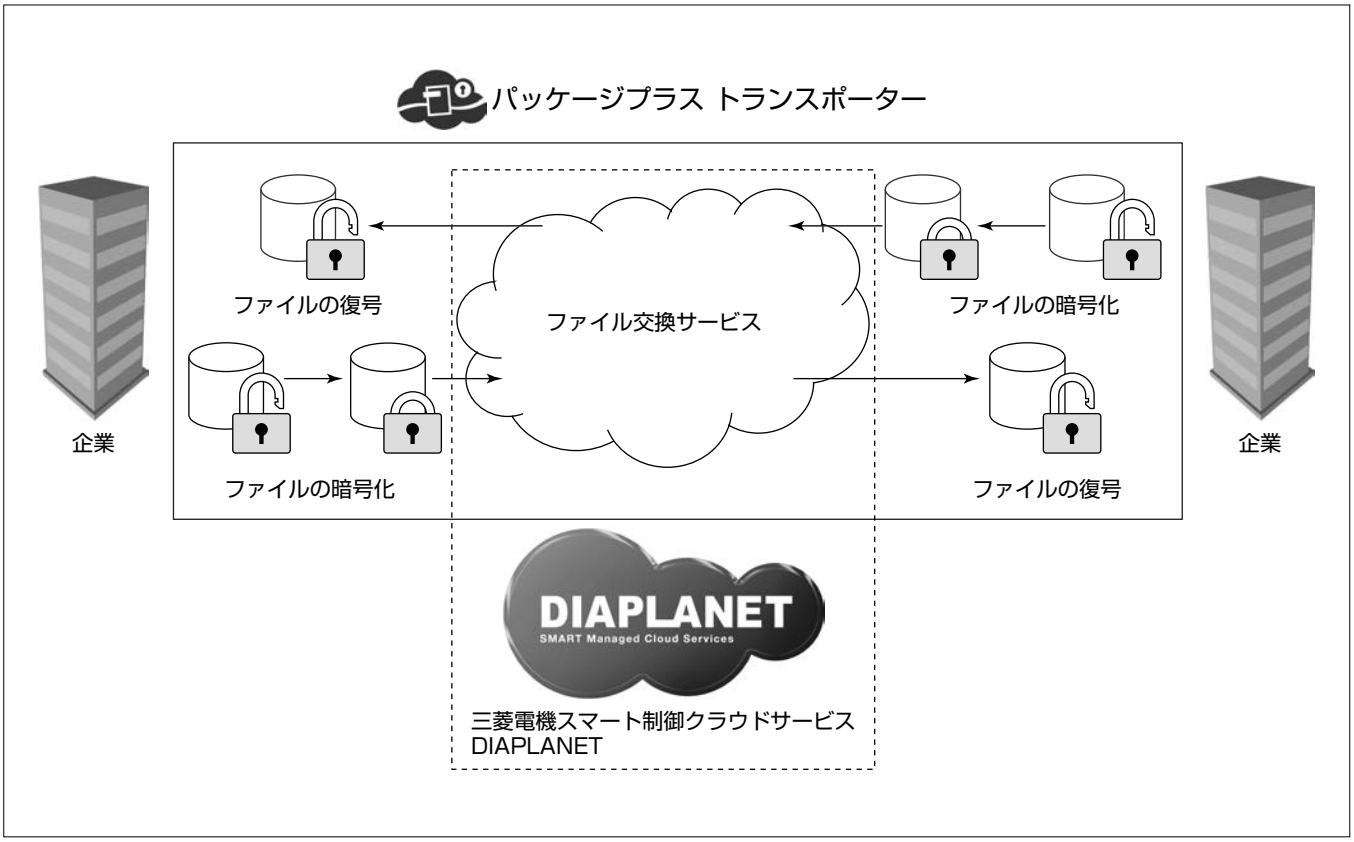
Takeshi Suzuki, Yusuke Watanabe

要　旨

㈱三菱電機ビジネスシステム(MB)は，機密情報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月から開始した。パッケージプラス トランスポーターは，三菱電機の“関数型暗号(1)”を実装した三菱電機スマート制御クラウドサービス“DIAPLANET(2)”上で企業間における機密情報ファイル交換を実現する。

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，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渡しは，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ため，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用した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

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上で提供している。これによって，安心・安全なファイル交換を実現している。

1. まえがき

企業間のデータの受渡しは，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。また，2016年１月から運用の始まった“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，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用したDIAPLANET上でファイル交換を実行するサービスであるパッケージプラス トランスポーターの提供を開始した。

本稿では，このサービスの機能と特長，及び他社サービスにない特長について述べる。

(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ある。

2. パッケージプラス トランスポーターの概要

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って，安心・安全な運用環境を“PaaS(Platform as a Service)”及び“SaaS(Software as a Service)”で提供する。パッケージプラス トランスポーターは，DIAPLANETの提供する“認証認可機能”と“暗号PaaS機能”を利用して企業間等の機密情報ファイルの交換を安心・安全に実現するサービスである。

このサービスでは，ファイル交換相手を設定する機能によって，指定した相手先だけが復号できるという堅牢(けんろう)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，このサービスでのファイル交換は，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)を組み合わせることで，機密情報をより強固に保護する仕組みを採用した(**図１**)。

(注２)　Windows は，Microsoft Corp. の登録商標である。

3. パッケージプラス トランスポーターの機能と特長

この章では，パッケージプラス トランスポーターが持っている，安心・安全に機密情報ファイル交換を行うための機能について述べる(**図２**)。

3.1　パッケージプラス トランスポーターを構成するツールと機能

このサービスは，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)”，利用元と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**のとおりである。

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のファイル交換を行うが，このサービスでは，**図３**に示すように利用元と複数の相手先との間でファイル交換が可能である。

利用元は，このサービスを契約した企業や部門であり，複数の相手先とファイル交換ができ，このファイル交換を管理する。相手先は，利用元とだけファイル交換ができる企業や部門である。

また，利用元側では，複数の担当者が利用できるように，担当者別に識別子(IDentifier：ID)を持つことができる。

3.3　ファイル交換ツール

機密情報ファイルを安心・安全に交換するためのクライアントツールである。用途によって，複数の相手先とファイル交換を行う利用元が使用する通常版と，相手先が使用

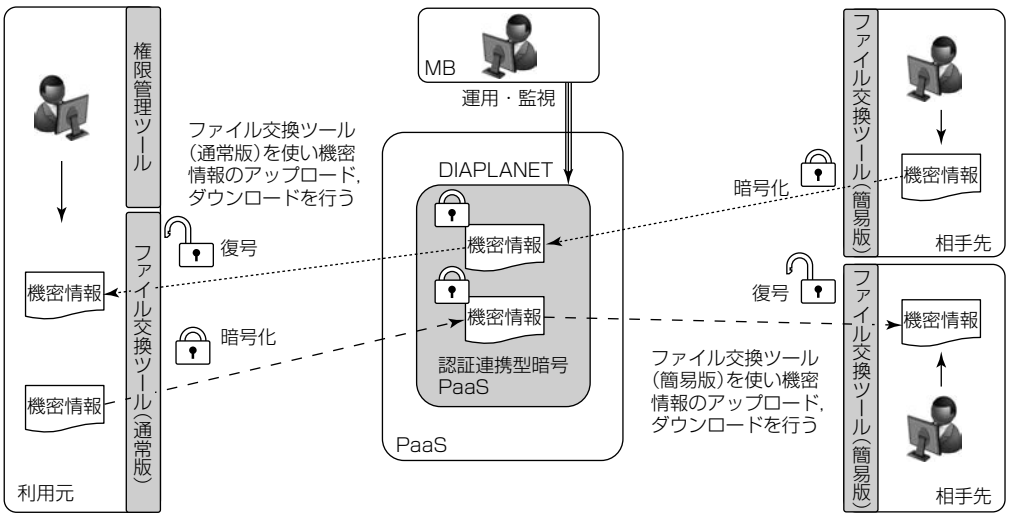


図１．機密情報ファイル交換サービスの概念図

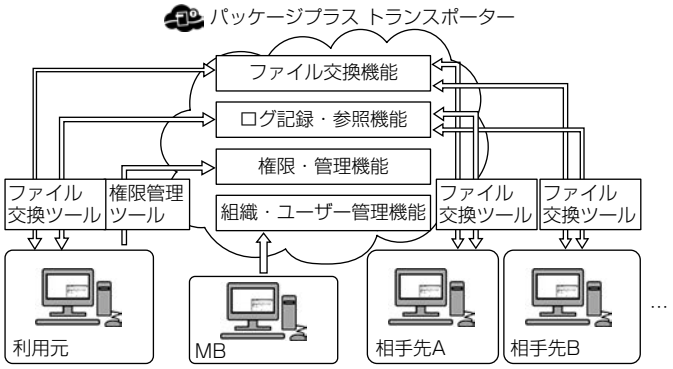


図2．機密情報ファイル交換サービスの機能

表1．機密情報ファイル交換サービスの構成ツール

	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		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	—	—
	フォルダ管理		

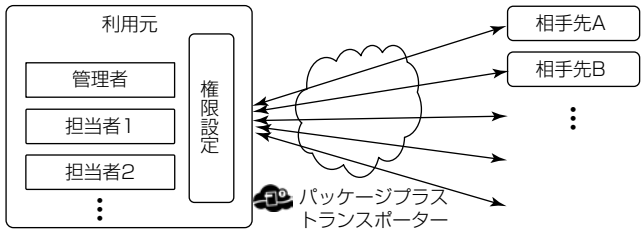


図3．利用元と相手先の概念図

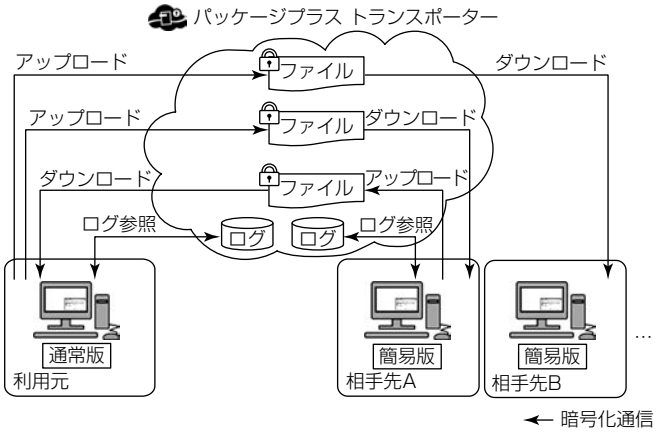


図4．ファイル交換ツール利用の概念

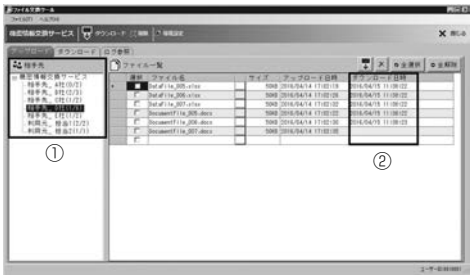


図5．ファイル交換ツールのアップロード画面例

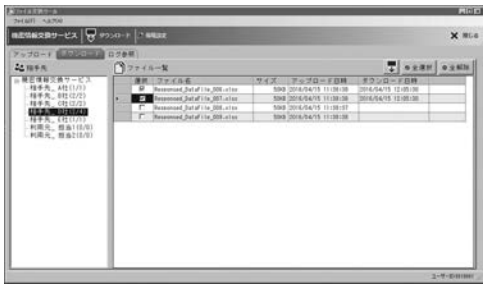


図6．ファイル交換ツールのダウンロード画面例

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交換もできる。

図4にファイル交換ツール利用の概念を示す。ファイルを相手先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このサービスの領域内にアップロードする。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をダウンロードする。

なお，簡易版はファイルの送受信先が1つの場合だけに使用できるように設定されており，操作を簡単に行うことができ，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5**①)，さらに相手先ごと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5**②)。

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，相手先ごとに表示される(**図6**)。それらのファイルは，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されるが，“環境設定”画面でのパラメータ設定によって，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**)。

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**)。

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

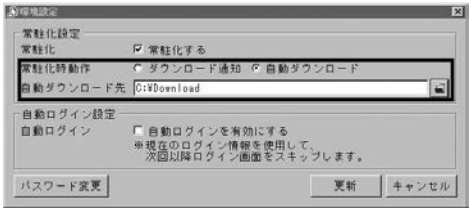


図7．環境設定画面

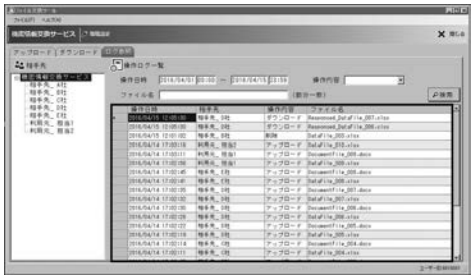


図8．操作ログ参照画面例

手先の名称や，利用元の名称，利用元の担当者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**)。また，“権限管理ツール”は，相手先からの要請等によって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。

3.5　組織・ユーザー情報の管理

この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**)。

3.6　他社サービスにない特長

⑴　機密性・完全性の確保

機密情報のファイル交換サービスは，暗号化通信によって通信経路を暗号化してファイルの送受信を行っている。万一暗号化通信に脆弱(ぜいじゃく)性問題が発覚してファイルが搾取されても，パッケージプラス トランスポーター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，この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**)。

⑵　個人情報を必要としない

このサービスでは，設定情報に個人情報がな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。自分宛ファイルが送信された場合，メールでの通知があれば便利であるが，このサービスでは，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，自分宛のファイルが送信された場合に，自動で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を持っている。

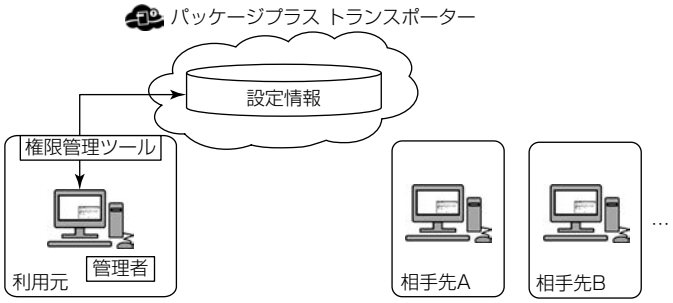


図9．権限管理ツール

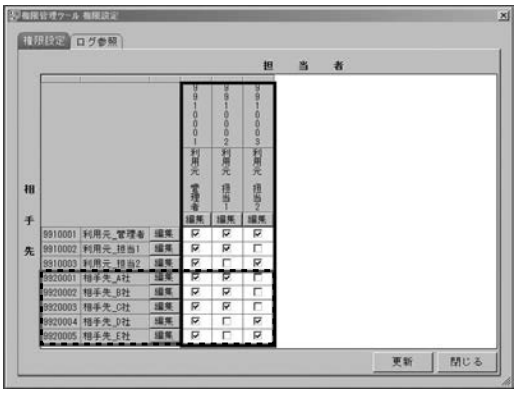


図10．権限管理ツールの設定画面例

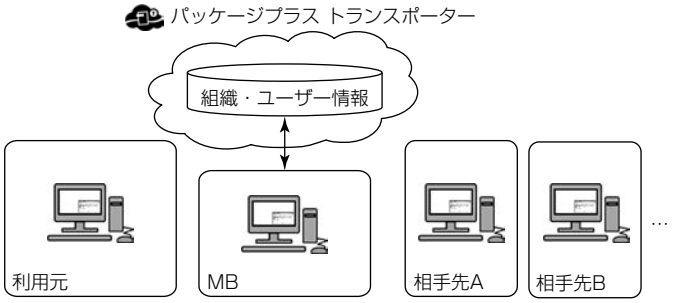


図11．組織・ユーザー情報の管理

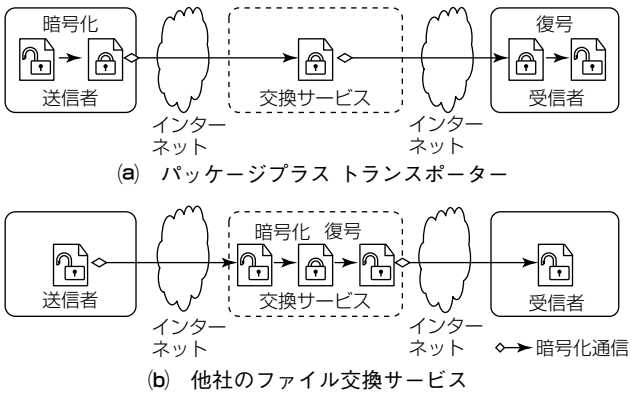


図12．ファイル交換サービスの比較

3.7　提供サービスの要件

このサービスが提供するサービスの要件は**表2**のとおりである。

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ごとにユーザーが指定

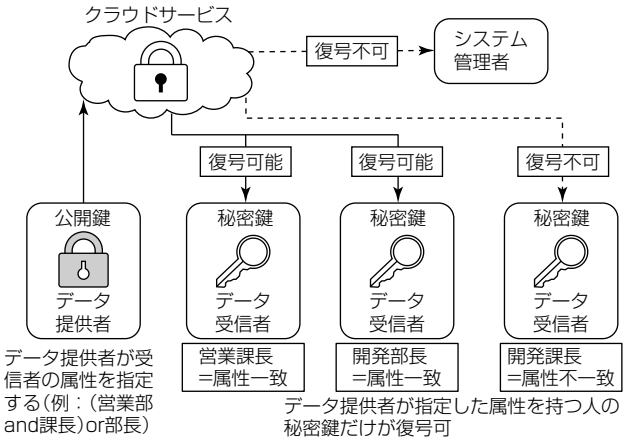


図13．関数型暗号のアクセス権限機能

4. 関数型暗号

関数型暗号は，三菱電機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更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だけでデータの復号を可能としている。これが関数型暗号の大きな特長である（**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，又は部長((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，人事異動等によって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。

先に述べたように組織情報と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

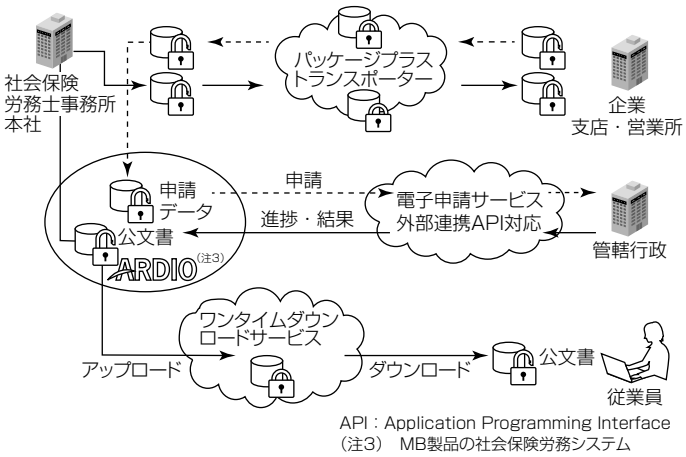


図14．パッケージプラスの機能全体図

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，パッケージプラス トランスポーターでは，利用元から相手先にデータ送信する場合は個人名宛に秘密鍵を送付する。逆に，相手先から利用元にデータ送信する場合は，個人名宛ではなく利用元の職名宛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用しつつ簡便に使用できるように考慮している。

5. むすび

今後もファイル交換の利用頻度は高くなることが予想され，より安心・安全なファイル交換等を行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4)，“eLTAX”(注5))等のファイル交換をより簡単に，より安全に利用できる仕組みを“パッケージプラス”の製品ラインアップとしてそろえ，安心・安全なファイル交換サービスをサポートするソフトウェアを提供していく（**図14**）。

（注4） 電子政府の総合窓口(e-Gov)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ある。
（注5） eLTAXは，一般社団法人地方税電子化協議会の登録商標である。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ある。

参考文献

(1) 三菱電機ホームページ：注目の研究・技術 関数型暗号
http://www.MitsubishiElectric.co.jp/corporate/randd/spotlight/spotlight15.html
(2) 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)
http://www.MitsubishiElectric.co.jp/corporate/giho/1601/pdf/1601007.pdf