［さようなら，意味のない暗号化 ZIP 添付メール］

2 PPAP のセキュリティ意義

楠　正憲 | 国際大学 Glocom

なぜか日本でだけ定着している PPAP

俗にいう PPAP とは，パスワード付き ZIP ファイルと パスワードを，電子メールで送付する方式を指す．組織によっては添付ファイルを自動的に暗号化 ZIP に変換する仕組みがメールシステムに組み込まれ，組織外に添付ファイル付きのメールを送信すると，自動的に暗号化 ZIP ファイルに格納し，ZIP ファイルとパスワードに分けて送信する設定となっている．こうした製品はメール誤送信対策ソフトと総称され，ヒューマンエラーによるメールの誤送信に対して一定の効果があると主張しているベンダもある．こうした誤送信対策ソフトは日本国内に限って，官公庁や金融機関をはじめとした大企業で広く導入されている．

例：https://www.lrm.jp/mailzipper/attachment-encryption/

PPAP の何が問題なのか

PPAP の基本的な問題は，暗号化 ZIP ファイルの送信・受信者ともに負担が重いにもかかわらず，通信の傍受に対して何ら防御の意味を持たないことである．暗号化する対象のデータと，そのデータを暗号化・復号化する鍵とを同じチャネルでやりとりしてしまうと，暗号化 ZIP ファイルを窃取できる攻撃者は，その復号化に用いる鍵を窃取することも可能となってしまうので，通信経路上での傍受からデータを保護するための暗号化としては何ら意味がない．

近年では PC だけでなくスマートフォンやタブレットでメールを送受信する機会が増えている．iOS や Android では添付ファイルをプレビュー表示する機能を具備しているが，出荷時の状態では簡単に ZIP ファイルを開けない場合があるほか，仮に開ける場合も暗号化 ZIP を展開するための操作は煩雑で，検索などの機能が適切に機能しない．

また，これらの障壁を乗り越えて暗号化 ZIP を展開できたとしても，日本語ファイル名が文字化けすることが多い．文字化けは PKWARE 社が設計した ZIP ファイルフォーマットの規格が，ファイル名の文字コードを規定していないことに起因する．一般に Windows の ZIP 暗号化ソフトは ZIP ファイルフォーマットの文字コードとして，non-Unicode アプリケーション向けの設定文字コード（日本語版であれば CP932 いわゆるシフト JIS）でエンコードするのに対して，iOS や Android アプリケーションは UTF-8 を前提にデコードする場合が多く，文字化けが発生してしまう．

PPAP がセキュリティ的に意味がなく，操作が煩雑なだけではない．近年のメールシステムでは，添付ファイルに対して詳細な解析を行っている．ウイルス対策ソフトによるシグニチャ型の既知のマルウェア検査に加えて，サンドボックス装置の仮想マシン上で添付ファイルを実際に開き，不審な挙動を行わないかどうかの確認などが行われる．暗号化 ZIP で送られてきた場合，同時に送信されたパスワードを使って復号して検査する機能を具備していない限りは，暗号化 ZIP 内のファイルについて検査が行われない．技術的には暗号化 ZIP と対応するパスワード通知メールとを解析して，ZIP ファイルを復号することも難しくはないはずだが，送信者が受信環境として前提にできるほど普及してはいない．

このように暗号化 ZIP ファイルとパスワードを同時に同じチャネルで送ることは，送受信者双方のユーザビリティを悪化させる上に，セキュリティ的には機密保護

の観点から何ら意味がなく，シグニチャ型のマルウェア対策やサンドボックスによる検疫を迂回してしまうことから，受信者に大きなリスクを負わせてしまうことになる．

最低限の機密性を確保できる暗号化 ZIP の運用とは

では，どのような電子メールの暗号化であれば，セキュリティを確保できるだろうか．実は暗号化 ZIP ファイルでも機密性を保つ方法がある．具体的には暗号化 ZIP ファイル本体のみを電子メールで送って，ZIP ファイルの暗号化・復号化に用いるパスワードは別経路で共有する方法だ．たとえば対面でのパスワード生成規則の事前共有，電話や郵送，SMS，ソーシャルネットワーク等の他経路を用いてパスワードを受け渡す方法が考えられる．相手の電話番号など他の連絡方法を知らず，電子メールによる連絡しかできない場合であっても，パスワードを平文でやりとりするのではなく，両者が共有している知識に基づく間接的な表現方法でパスワードを表現することによって，それなりに機密性を確保できると考えられる．

この方法のメリットは仮に暗号化 ZIP を間違った相手に誤送信してしまったとしても，誤送信先との間でパスワードを共有していなければ，受信者が容易には解読できないことだ．暗号化 ZIP ファイルとパスワードとを別チャネルでやりとりする場合，両方を誤って同じ相手に送ってしまうリスクは小さい．このことが暗号化 ZIP ファイルを利用することで誤送信対策になるという認識に繋がり，ISMS や P マークの審査において「個人情報を含む添付ファイルを取り扱う際に，セキュリティ対策（データの暗号化，パスワード設定など）の措置を講じること」（情報サービス産業協会 2010 年）といった規定が設けられるようになったと考えられる．
https://www.jisa.or.jp/service/privacy/tabid/831/Default.aspx?itemid=31

こうした規定が各組織のセキュリティポリシーに追加されて，かかる規定を確実に遵守させる方法として，外部アドレス宛の電子メールについて，添付ファイルを自動的に暗号化するソリューションが普及したと考えられる．しかしながら誤送信対策として暗号化 ZIP が有効なのは，誤送信先が復号のためのパスワードを知らないことが条件となる．システムによって自動的に暗号化 ZIP ファイルとパスワードを送付してしまっては，この条件を満たすことができない．こうしたシステムを使って，暗号化 ZIP とパスワードを同一チャネルで送ってしまっては，メールの誤送信対策としてはまったく機能しない．こうした仕組みをメールの誤送信対策として採用している組織は，セキュリティポリシーが形骸化してしまって，適切なリスク管理を行えていないことが推定される．

暗号化 ZIP 以外の安全なデータの受け渡し

これまで電子メールの暗号化にあたっては，暗号化 ZIP よりも優れた方法が考案されてきた．公開鍵暗号方式によって共通鍵を交換する方法として，古くは 1991 年，Phillip Zimmermann が PGP (Pretty Good Privacy) を発表している．この方式は 1996 年 RFC 1991 PGP Message Exchange Formats として標準化されて，後に RFC 2440 を経て RFC 4880 と更新されている．PGP では鍵管理を利用者自身が行う必要があり，暗号や PGP について，ある程度の専門知識が必要となる．PGP はオープンソースソフトウェアの開発や，ソフトウェアの脆弱性報告などに使われている．

利用者による鍵管理を必要としない方式として，認証局が証明書を管理する PKI を利用する S/MIME が RSA Data Security によって開発された．S/MIME は Microsoft Outlook をはじめとした多くの電子メールクライアントに採用されて，一時は暗号化メールの本命と目されたものの，署名・暗号化に用いる電子証明書の価格が高止まりしたため普及には至らなかった．その後 Hotmail や Gmail などの Web メールの流行，ス

マートフォンの普及でスマホ用メールアプリで S/MIME 対応が進まなかったことから，普及のタイミングを逸してしまった．

暗号化メールは通信路の暗号化には有効だが，正規の受信者が復号したデータを第三者に転送することを防ぐことはできない．このため 2000 年代に入ってからは，電子メール自体を暗号化するアプローチから，メールを転送されても正規の受信者しか開けないように，DRM 技術を用いて暗号化に使う鍵管理を集約する製品が登場した．たとえばマイクロソフトは Office IRM (Information Rights Management) を Microsoft Office 2003 から導入した．Office IRM はディレクトリサービスや文書管理サーバの権限管理と連動して，メールの転送や印刷も含めて制限できる．しかしながら他社製品との相互運用性に欠け，組織間で運用するには多くの課題があった．

添付ファイルからクラウド上でのファイル共有へ

2010 年代に入り，電子メールに MIME でファイルを添付するよりも，クラウド上でファイルを共有して適切な権限管理を行うことが，適切に文書管理する方法として定着した．Box などのストレージサービスが組織間のデータ共有方法として広く使われ，Google が Web 上で複数人で単一のファイルを開いて同時に編集できる機能をリリースして Microsoft も追随した．ID フェデレーションとクラウドサービスの普及によって組織を超えた ID 管理と連動した権限管理が当たり前となって，メールにファイルを添付するのではなく，組織を超えてクラウド上でファイルを共有して，必要な者にアクセス権限を付与する方法が普及した．

このように複数組織がクラウド上で単一のリソースにアクセスする方法は，電子メールの添付ファイルとして暗号化したファイルをやりとりする方法と比べ機密を保持する上でメリットが大きい．いちどデータを相手に送ったとしても，いつでも事後的にアクセス権限を剥奪できる．データ自体を送った場合は復号化した後のデータの印刷や転送を禁止できないが，クラウドサービス上のデータにブラウザからアクセスできる権限を付与した後も，印刷や転送の権限は個別に制御できる．

電子メールの添付ファイルからクラウドサービスへの移行にはほかにも理由がある．Windows では添付ファイルを開くアプリケーションを呼び出す際 DDE と呼ばれる仕組みが使われるが，文書ファイルに偽装してマクロや実行ファイルを実行させることを防ぐことが難しい．iOS や Android ではプログラムとデータを分離して取り扱うが，Windows は後方互換性のためにメールの添付ファイルを実行できてしまう仕組みが残されており，今でも標的型攻撃に悪用されがちだ．これを防ぐためには iOS や Android のようにファイルの閲覧とプログラムの実行とを明確に分けて，プログラムごとにアクセスできる資源を分離する必要があるが，後方互換性との両立は難しい．

もちろんクラウドを通じたリソース共有にも課題はある．各クラウドサービスの ID が厳格に管理されていることが前提で，フィッシングによる ID 詐取や，誤って攻撃者のリンクを踏んだ場合のトークン窃取などに対して対策が必要となる．多要素認証や，安全なトークン管理などを通じて，ID を厳格に保護することが重要だ．しかしながら従前の添付ファイルと比べて，データの集中管理と，資源管理の厳格な分離を実現することは容易と考えられる．

電子メールからビジネスチャットへ

クラウド時代に入って変化したのはファイルの共有方法だけではない．メッセージのやりとりも，電子メールではなくチャットが広く使われるようになった．この動きは法人よりも先に個人で起こっている．米国では 2002 年に LinkedIn，2003 年に Friendstar が登場，日本では 2004 年に Gree と mixi が登場，その後 Facebook，Twitter など高いシェアを持つ SNS が登場したことで，個人間のコミュニティがメーリングリス

トからソーシャルネットワークに移行し，SNS に組み込まれた個人間通信でのコミュニケーションが広がった．

この流れを決定的にしたのがスマートフォンの普及とともに流行した KakaoTalk, LINE, Whatsapp といったメッセンジャーアプリだ．こうしたチャットアプリは電話帳を元にソーシャルグラフを形成して，知り合い同士のコミュニケーションを容易にする．電子メールと違ってチャットアプリでは知り合いとしかメッセージのやりとりをせず，悪意ある第三者が紛らわしいメッセージを送ることが難しい．やりとりの開始にあたっては，利用者の明示的な許可が必要となる．また電子メールと異なり個別システムが縦割りで閉じていることが前提で，標準化を待たずサーバとアプリのプロトコル変更が容易となる．

これらのチャットアプリは利用者が通信相手を明示的に管理しているので，これらを鍵管理と連動させることで，容易に暗号化を実現できる．日本で広く使われている LINE や Facebook Messenger，Apple の iOS に標準で組み込まれている iMessage，ロシアが遮断を試みて失敗した Telegram などは，E2E 暗号化 (End to End Encryption) を実現しているとされる．E2E 暗号化によってサービス提供者がメッセージを傍受することが難しくなることが期待されるが，いずれもオープンな実装ではなく，鍵管理をサービス事業者に委ねていることから，安全性を外部から検証することは難しい．

消費者向け SNS に遅れて企業向け SNS が数多く登場し，ビジネスチャットへと発展した．2009 年にリリースされた Yammer は 2012 年マイクロソフトに買収され，2011 年には日本で Chatwork が，2013 年には西海岸で Slack が登場している．買収した Yammer を Office 365 の一部として提供していたマイクロソフトは 2016 年 Teams を発表してビジネスチャットとビデオ会議を統合した．

これらビジネスチャットが特徴的なのは従前の組織単位の情報システムではなく，組織をまたいだプロジェクトのメンバ間のコラボレーションを支援していることだ．電子メールやファイルサーバが企業単位で整備されて，標準プロトコルを使って組織間を結ぶ方式だったのに対して，ビジネスチャットは単一のクラウドサービスとして提供されて，組織を超えたプロジェクトのメンバに対して安全なサービスを提供する．ビジネスチャットだけでなくさまざまなクラウド上の SaaS が ID Federation と API で結合して，組織を超えてシームレスにサービスを構築できる時代がきた．

従前の電子メールがメールサーバ，メールクライアント，認証局の間で三すくみとなって安全で使い勝手の良い暗号化メールを提供できない間に，SNS やチャットアプリ，ビジネスチャットが一気通貫で ID・クラウドサービス・各 OS 向けアプリを提供して世界で広く使われるようになった．取り残された電子メールの世界で，使い勝手の悪い暗号化 ZIP が日本では細々と使われ続けてきた．

取り残される日本の「セキュア」な組織

残念ながら PPAP が残っているような会社では，こうしたクラウドサービスを使うことが難しい場合が多い．たとえば情報漏洩対策として Office 365 や G Suite, Slack などはフィルタリングされ，ブラウザ仮想化によって複雑な Web アプリはまともに動かず，情報を端末側に残さないためにシンクライアントを使っていて，常に画面の動きがモッサリとしていたりする．

そういった組織でも外部とのやりとりはあるので，シャドー IT として私用スマホで Gmail や LINE, Dropbox が業務に使われる．昨今の新型コロナ対策のような大規模のテレワークは想定されておらず，VPN の帯域が逼迫して，整備したつもりのテレビ会議システムが適切に機能しない．迷惑メール対策は厳重に行われ，サンドボックス装置も入っているが，他社から暗号化 ZIP が送られてきても復号できず十分に機能しない．暗号化 ZIP にファイル名を文書ファイルのように偽装した実行ファイルを仕込むと簡単に引っかかっ

てしまう．

このようにルールと仕組みがチグハグなまま何を守っているか分からなくなってしまったのは日本固有のITガバナンスも影響していると考えられる．日本における情報セキュリティは2001年のCodeRed・Nimdaウイルス流行，2003年のBlasterウイルス流行に続いて，2005年に個人情報保護法が完全施行されたため，当初は制度対応として進められてきた．組織規定の整備は専門家ではないローテーション人事の中で継ぎ接ぎに行われ，セキュリティ・ソリューションはインシデントのたびにベンダ提案として再発防止策として積み重なり，リプレースの際にも外すことのリスクを判断できず，どれも廃止できないために，多数のソリューションが複雑に絡み合う．その中で見当違いのメール誤送信対策としてのPPAPは生き残り，従前の情報漏洩対策の前提と矛盾するクラウドサービスは遮断せざるを得ない．

そういった組織であっても，社外とのコラボレーションやデータのやりとりは頻繁に発生するため，業務を回すためにシャドーITが横行し，監視が難しい暗号化ZIPの添付ファイルが飛び交う．あちこちで微妙にバージョンが異なるファイルが散在し，印刷や外部への転送を止めることができない．個人情報漏洩で社会面に載ることに怯えてConfidentialityばかりが肥大化し，IntegrityやAvailabilityを脅かす他のリスクと真剣に向かい合ってこなかった組織の末路だ．

組織を超えた共同作業と業務継続の確保へ向けて

1990年代LANとイントラネットの普及当初は，部門単位でネットワークが構築されてきた．2000年代前半にブロードバンド常時接続の普及にセキュリティ対策が追いつかず，世界規模でBlasterウイルスの爆発的感染を招いた．日本では個人情報保護法の施行とも相俟って情報漏洩対策を全社的に推進するため，部門単位ばらばらに整備されたITから，全社規模のITへと統制を働かせるように改革が進んだ．

しかしながら伝統的な組織の多くはジェネラリスト中心のローテーション人事で専門家を育てず，規程類はローテーション人事で継ぎ接ぎを重ねて，セキュリティ対策はベンダ任せでインシデントのたびに再発防止策の積み上げで整備してきた．その結果いざ新型コロナウイルスの爆発的感染で在宅勤務への急速な転換が必要となったとき，円滑に機能しない硬直的なシステム，使い勝手を犠牲にしながら大して安全ともいえない不便なシステムができあがってしまった．

新型コロナ対策による前例なき長期に渡る大規模な在宅勤務の継続を経て，これまで整備したインフラがうまく機能しなかった組織は，数年かけてITシステムの総点検を行う必要が出てくるのではないか．非対面でも社内外と円滑に共同作業を実施できる情報システムの実現のために，Blaster・個人情報保護法施行を契機に日本の組織が積み上げてきた情報セキュリティ対策をゼロベースで見直して，目的と手段をセットで再構築する必要が出てくる．

具体的なリスクを洗い出して実効的な対策を打つためには，システムとして従前の境界型セキュリティを見直すだけでなく，規程類の整備とシステム構築を一体的に検討できるように，プロパーとベンダとの関係や役割分担も見直す必要が生じる．PPAPの不条理は見直すべきITシステムを取り巻く矛盾の一端にすぎない．

（2020年4月5日受付）

■楠　正憲（正会員）　masanork@gmail.com

マイクロソフト，ヤフーなどを経て2017年からJapan Digital Design CTO．内閣官房 政府CIO補佐官としてマイナンバー制度を支える情報システム等の構築に従事．