［さようなら，意味のない暗号化 ZIP 添付メール］

4 座談会「社会から PPAP をなくすには?」

崎村夏彦 | NAT コンサルティング　大泰司章 | PPAP 総研
楠　正憲 | 国際大学 Glocom　上原哲太郎 | 立命館大学

PPAP の定義

崎村：さて，本日は「社会から PPAP をなくすには?」というテーマで座談会を行いたいと思います．アジェンダですが，PPAP の定義，PPAP 賛成の論拠への反論，より良い方策を議論します．まず PPAP の定義ですが，オフラインで鍵を共有するのも PPAP だと思っている方もいらっしゃるようなのですけれども，それは違いますよね．

大泰司：1 通目に ZIP を暗号化して添付ファイルを送って，2 通目でパスワードを送るというやり方です．2 つの軸があって，パスワードを同じ経路を送るか，違った経路で送るか．もう 1 つは，すべての添付ファイルを暗号化するか，自分で判断して特定のファイルだけ暗号化するか．自動で添付ファイルを暗号化して送るソリューションを使うと，すべての添付ファイルを暗号化し，同じ経路でパスワードも送信することになる．これを，この議論では PPAP と呼びたいと思います．

上原：この議論では，暗号化 ZIP が送られて，すぐそのあとにパスワードが追いかけていくスタイルに限るということですよね．

PPAP 賛成の論拠への反論

誤送信防止

崎村：PPAP の定義は分かったので，PPAP 賛成の論拠への反論を挙げていきたいと思います．

上原：PPAP 賛成派の意見には何があるのでしたっけ．

大泰司：手動で送って，2 通目までの間に間違えたなと気が付くケースがあるというものです．

上原：それだけを論拠に頑張っているんですかね．自動の場合はまったく意味がないですよね．

大泰司：ないですね．ただ，多くの場合はこのソリューションを誤送信防止ツールと銘打って売ってます．送る前に，本当にこの宛先でいいですかとダイアログが出てきて，OK，OK，OK とクリックしないと送信されない．大体この機能が入っています．

上原：それは，添付ファイル暗号化とは関係ないよね（笑）．送信前にメーラーでメールアドレスを確認する機能を付ければいい．

楠：この問題は根深くて，本当にいちいち OK を押さなければいけないし，そのあと保留され，さらにメール上，リンクを組んでどこかのページで挿入をするみたいなフローが入っていたりする．

　あとは，会社によっては，上司を CC に入れないと添付ファイルを送れずに，自分だけで送ろうとすると自動的に止まるとか，いろんなバリエーションがある．

上原：上司の承認を得るために，上司を CC に入れ，CC に入っている上司が OK を押さないとメールが出ていかないというのは，それはそれでガバナンス上，意味はなくはない．だけど，それは添付ファイルとは関係ない気がします．

崎村：添付ファイルあるなしでリスクが異なるという

のはあり得ます．だから上司がもう1回，その添付ファイルが正しいかどうかを確認するのはありかもしれない．

以前，知っているケースでは，ちゃんとPDFにした見積書を提出しなければいけないのに，Excelをそのまま添付してしまって，中のコスト構造やなんかが全部ばれてしまった．上司が確認したくなるというのも分からんでもない．でも，PPAPとはまったく関係ないですよね．

上原：そうだと思うのですよ．だから少なくともZIPで暗号化するのというのは相手にコストをかけているだけなので，まったくセキュリティ上の意味はないですよね．

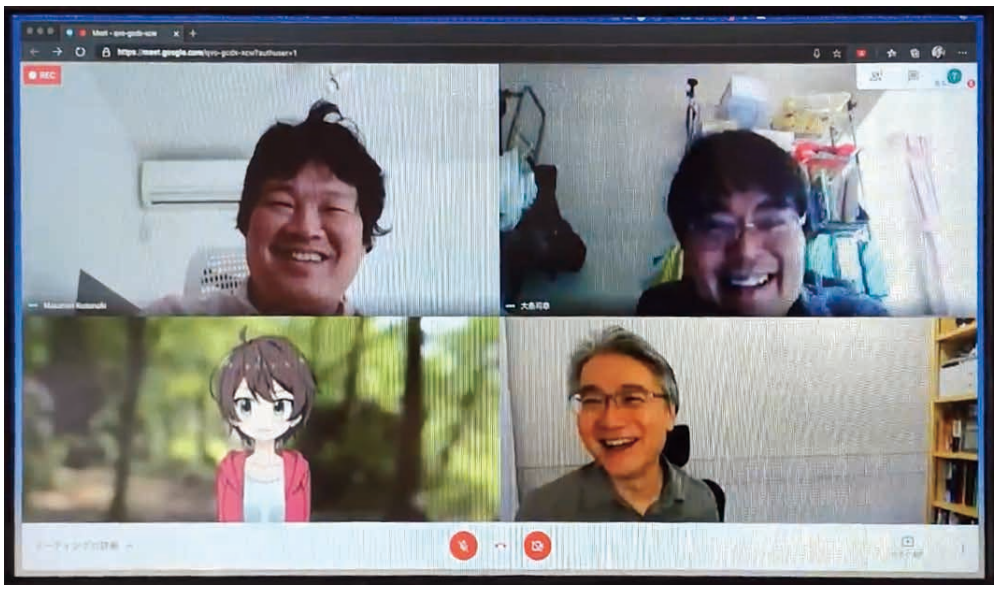
崎村：ないと思います．あと，誤送信防止ということだと，僕，実は2005年ぐらいに社内のR&Dでプロトタイプをつくったことがあります．実際には運用されなかったのですけど．まず，メールの最初の3行に相手の所属と会社名と名前を入れる．メールを送信するとゲートウェイがその最初の3行を読んで，会社名とドメインとをマッチさせ，マッチしないと本人にメールがきて，ドメインがマッチしないけど本当にいいですか?と確認をとるというものです．

大泰司：それと同じようなシステムについて，誤送信防止システムを出しているベンダさんから相談がありました．それで，日本のすべての会社のドメインリストを提供してくれないかと言われたのだけど，それはできなかった．

崎村：大きな会社だと大抵取引先登録をしているので，そこからドメインを引っ張ってくればいいと思ったのですよね．あと上場企業だったら当然引っ張れるし．技術的には可能で，メールを送れなくするわけではなくて，本当にドメインがマッチしないけどいいんですかと確認するだけだから．いや違っていてもいいんだといってやれば，それはそれで問題ない．

上原：誤送信で一番多いパターンというのは，たとえば，メーラーがアドレス補完機能を持っていて，立命館大学の上原にメールを出すときに，宛先にueharaまで打ち込んだら補完されて，そこでエイヤーと出してしまうと，実は全然違うコンプリーションしていて，まったく違う人に送信してしまうパターンなのではないですか．誤送信防止の人たちが主張しているのはほかにどんなパターンがあるのですかね．

楠：たとえば，ルール上，組織以外は全部BCCに入れなければいけないのに，CCに入れて，個人情報



■座談会の様子
左上：楠　正憲
左下：上原哲太郎
右上：大泰司章
右下：崎村夏彦

漏洩になってしまうケースとか.

上原：でもそれもPPAPと関係ないね. CCをチェックすればいいわけですよね.

楠：そういう機能も入っていたりします.

崎村：アドレスの補完機能があるからこそ誤送信が減ると考える人たちもいるわけですね. ただ，皆さん失敗からしか学ばないので，補完機能で誤送信したということがあると，3カ月後ぐらいに補完機能が使用禁止になったりする.

間違ったPDCA (Plan-Do-Check-Action) が日本中をまわっていて，基本的にその機能がなくしたミスというのはミスとしてカウントされない. あらかじめ登録してある，相手が分かっている，謝れば済む相手しか補完されないはずなのに，その補完機能をオフにしていると全然訳の分からない人に送られてしまうというのがある.

取引先として登録してある人だったら，もう面が割れて，たぶん知っている人だから，間違って送ってしまった，ごめんなさい，で済んでしまうわけですよね. しかし，まったく面識のない人に送られてしまって事件になるリスクを考えると，後者の方が実はリスクの度合いとしては大きいような気がするのですけれども.

ISMSやPマークが要件としているという都市伝説

上原：やはり，こう，納得感がある理由がないのに何でこんなに使われているのですかね.

崎村：人によっては，ISMS (Information Security Management System) が要求するからとか，Pマーク (プライバシーマーク) が要求するからとか，そういう都市伝説があって，その都市伝説に従って実装している人たちも結構いるみたいです.

上原：Pマーク説は結構あちこちで聞きますよね. それで，大泰司さんは結局その犯人捜しはしたんでしたっけ.

大泰司：犯人捜しして，見つからなかったのですよ.

上原：やはり見つからなかった.

大泰司：ただ，誤送信防止のソリューションを出しているベンダがPマークの審査基準がこう改定されているから，これに対応しなければいけませんというようなことは書いていますね. では本当にPマーク審査の現場でどうなっているのか聞いてもらったけれども，分からなかったです.

それで，JIPDEC (一般財団法人日本情報経済社会推進協会) の中に教育用・研修用資料としてガイドラインのようなものがあったのですが，それを見たら，個人情報は暗号化しましょう，そのファイルを送ったときにはパスワードは別の手段で送りましょうと書いてある.

上原：別の手段とは書いてありますね.

楠：うん. 正しい.

上原：別の手段だったら正しいのですけれども，別の手段というのが同じ手段のメールにいつの間にか化けているということですかね.

大泰司：うん. そうですね.

崎村：審査基準の中に，個人情報を送るときは暗号化，安全管理措置をとることとは書いてある. でも，キーを同時に送っていたら安全管理措置として崩壊している.

楠：ただ，そこまで中身を見ない，チェックリスト式のセキュリティの人たちというのは，自分の頭でリスク評価をできない人が多くて. 対策しているかどうかと，その方法は社会で使われている実績ある方法かという，この2つを気にしている. 確かにPPAPはこれを非常によく満たすいいソリューションなんですよね.

上原：本当に広く，セキュリティを売りにしておられる大上場企業さまがお使いなので困ってしまう.

楠：たまによく訓練された日経BPの編集者なんかだと，ZIPはメールで送ってきて，パスワードはSMSかFacebookメッセージで送ってくる人はいますね.

崎村：それは正しい.

上原：まあ，正しいは正しいですね.

崎村：だから僕がもしパスワード付きZIPをやるのだったら，頻繁にやりとりする相手だったら，あらかじめ

両者で秘密鍵を決めておいて，それで送るようにすればいいですよね．

楠：私の働いている保秘を大事にする某所ではまさにそのやり方を使っているのですが，プロジェクトの数だけ約束事があると，最終的に破綻するのですよ．もうね，何カ月かおきに同僚に頼んでポストイットに書いてもらうという儀式が（笑）．

崎村：ただね，PPAP のほうが相対的に楽というのは，なぜかというと効果がないから．

PPAP に代わる安全な方式

SMTPS の強制

崎村：さて，では PPAP に代わる安全な方式の議論したいと思います．

上原：相手との SMTP の経路が SSL 対応になっているのだったら，もうそのまま送ればと思っています．安全という意味では十分安全．いまは通信区間にセキュリティリスクはあまりない．むしろ末端がこわい．マルウェアやフィッシングで ID を取られ，メールボックスの中を盗み見られていることのほうが問題．そっちを守ることにエネルギーを使うべき．経路のことはあまり気にしなくていいんじゃないか．

崎村：何を守ろうとしているかという部分ですよね．経路の安全性と到達先での安全性と 2 つある．あと PPAP な人たちがよく言っている誤送信防止．

上原：誤送信防止対策は別の方法でやるべき．G メールは送信ボタンを押してからしばらくは取り消せるようになった．PPAP で送ってから気が付くと主張する人たちは，このことをどう思っているのかなと．確かに僕も気が付くことがあるのですね，あっ，しまった，送り損ねた，戻そうみたいなのはたまにある．でも逆に言うと，あれで十分じゃんと．それが 1 つ目ですね．

事前鍵交換共通鍵暗号化ファイル添付

崎村：次に，事前鍵交換の共通鍵暗号化ファイル添付．本来の PPAP の在り方としては，あらかじめオフラインで共通鍵を交換しておいて，以後，その鍵でファイルを暗号化してメールに添付する．そうすると，鍵の長さが十分であれば，強度は十分となる．そもそもの誤送信対策で，元々やられていた本来の暗号化 ZIP の使い方．相手との間で事前に共有した鍵があるから，それ以外のところに送っても大丈夫，だから誤送信対策としても機能する．

楠：それこそが本来の誤送信対策なのですよ．

上原：ただ，十分長くて複雑な鍵じゃないといけない．某役所の仕事はこの事前共有鍵方式．UX 的にはしんどい．

楠：プロジェクトとか，研究会の数だけ覚えるのはまず困難．

崎村：こういうのは 1Password みたいなパスワード管理ソフトを使うしかない．

大泰司：またはモニタのまわりが付箋だらけになると．それでも分からなくなるから，前は部下に開けてもらっていました．

崎村：1Password は企業モードがあって，こういうシークレットキーを複数人でシェアできる．まさにそういうためのものではないかと．

楠：その問題を公開鍵暗号でクリアしてくれて僕らは幸せな時代を生きているはずなのに，なんでこんなにシェアードシークレットのハンドリングにこの 21 世紀に苦労しているんでしたっけ．70 年代にシャミアさまとかが解いてくれた大事な問題なはずなのだけれども．

公開鍵暗号化ファイル添付

崎村：その流れだと，次に出てくるのが公開鍵暗号化ファイル添付，アリスとボブがそれぞれの公開鍵を一定の場所に公開しておいて，その公開鍵を使ってファイルを暗号化して．PGP とか．

上原：PGP の鍵を公開しておいてやりましょうというのは，たとえば，IPA の届け出がその方式ですよね．

楠：PGP を使えないと届け出ができないというのはな

かなかすごいハードルが高い感じで.

崎村：UI（User Interface）や, Windows や Mac に最初から入っていないなどの問題ですよね. 逆に言えば, 皆が持っていて, UI も良いという状態になれば使えるということではある. エストニアは ID カード配布と同時に署名・暗号化のためのソフトを配っています.

公開鍵メッセージ暗号化（S/MIME）

上原：私はまだ細々と S/MIME で抵抗を試みています. 私のメールは S/MIME 署名されているのですけれども, この S/MIME 署名している鍵はどこにあるかというと, G さまが保管しておられます（笑）.

楠：G Suite ですか.

上原：そうです. G Suite の中でやっています.

崎村：私もやれるのですけれども, やって意味があるのかどうか（笑）.

楠：だいぶ哲学的な問いですよね.

上原：ええ.

崎村：多くのメーラーが, 特に携帯など, S/MIME で暗号化されてきているメッセージは読めない.

上原：暗号化は読めないですね.

楠：添付ファイルが読めるか微妙な感じ.

崎村：本文が表示されなくなってしまったとか.

上原：smime.p7s だって「ウイルスみたいなファイルが付いているけれども, 何ですか」というお問合せをいただく（笑）. あるいは, ゲートウェイで削除しましたというメッセージ付きで向こうに届くとか（笑）.

大泰司：サニタイズされてしまうのですよ.

上原：そうなのですよね. まあでも S/MIME はやればやるほど普及しない理由はよく分かってしまって（笑）. 昔はファイル名に日本語が交じると正規化アルゴリズムの実装が微妙に異なっていて, 検証が失敗するとか互換性問題があった. それはだいぶ解決したのですが, 一方で鍵管理の問題が解決しない. 私は S/MIME で届いたメールが暗号化されていたら IMAP（Internet Message Access Protocol）の Inbox に復号した状態で保存してほしいと思うのです. 暗号化したまま置いていると, その古いファイルを取り出すために自分の古い証明書をずっと持っておかないといけないから. でも, これがすごく難しい. そういううまい UI を提供してくれているメーラーがない. 署名にしても, 古い証明書をずっと履歴管理できるメーラーじゃないと昔のメールの署名確認に困る. なので, 両方の意味で, S/MIME はちょっとつらいのは実情かなと.

楠：やはり鍵管理そのものが人類に早すぎたのではないかと. 鍵管理というのはやはり難しい.

崎村：でも, だとすると, 暗号というのはすべての問題を鍵管理の問題に置き換える話・技術だから, 暗号化は無理筋という話になってくるわけですね.

楠：まあだからよろしく GAFA（Google Apple Facebook Amazon）に守ってもらおうという流れになってしまう.

上原：それで, その古いメールを取り出すたびに思うのですけれども, さっきの楠さんの話ではないですけれども, なんで S/MIME というのは 1 年ごとに証明書を更新しなくてはいけないんだっけと思うわけですよ（笑）.

大泰司：今, 3 年. 今度 2 年になったのかな.

上原：だんだん縮んでいっているので.

大泰司：特に暗号化に期限の短いものを使う必要は全然なくて, 署名のほうはまあしょうがない. 実際に使っていると S/MIME の暗号化はすごい楽ですよ. もう普段, 意識していないぐらいに.

上原：ただ, S/MIME の暗号化で普段, 意識しないとおっしゃるのはすごくよく分かるのですが, 意識せずに使えるというのは実は逆にネックになっているような気もしていて, ちゃんと自分は暗号化して送れているのかとか, 暗号化したものをちゃんと受け取ったのかというのをちゃんと確認する習慣を削いでいくような気がするのですよね. それはそれでいいのかみたいな気がして.

DNS を使った ID ベース暗号

上原：一応そこもですね，私，ささやかながら抵抗を試みていて．学生さんにつくってもらって情報処理学会の研究会で発表したのですが，DNS（Domain Name System）ベースの公開鍵暗号をつくっています．公開鍵というか，いわゆる ID ベース暗号なのですが，ID ベース暗号の公開パラメータをドメインごとに DNS で公開する．そうするとその DNS の管理がちゃんとしている限りにおいては，そのドメインで使っている ID ベース暗号のパラメータは DNS で入手できるから，それを使ってお互いにやりとりができる．有効期限の議論は，危殆化したことをドメインのほうが認識するまではエクスパイアしないという（笑）．そういう運用ルールで考えていて，危殆化したら DNS の鍵を入れ替える，その代わり古い鍵はあるルールで残して公開を続けるみたいな，そんな仕組みで設計しているところなのです．

メールのセキュリティというのは，S/MIME の普及が進まない間に別の方向に進化していて，PKI（Public Key Infrastructure）では SMTPS，POPS，IMAPS などの転送レイヤだけうまく技術が普及している．それより上位レイヤは，DKIM（DomainKeys Identified Mail）など，ひたすら DNS に頼っているわけです．

楠：SPF も含めて．

上原：SPF（Sender Policy Framework），さらに DMARC（Domain-based Message Authentication, Reporting and Conformance）ができて，それで今度，トランスポート層が SSL に強制されていることを MTA-STS（Mail Transfer Agent Strict Transport Security）で公告するようになってと．全部 DNS に頼っていて，それをみんな信用できているのだったら，DNS に残ったリスクというのは，みんな目をつむれるのかなと．今の PKI は DNS を信頼できないものとして扱いますけれども，DNS を信頼する公開鍵暗号系を標準化できないのかなというのは今ちょっと思ってて．

楠：結局 PGP が流行らなかったのは公開鍵の交換のところで，これをキー・サーバをつくるのではなくディレクトリをと考えたとき，インターネットでグローバルにスケールしているディレクトリは DNS という話に間違いなくなりますからね．

上原：そうなのですよね．キー・サーバがまったくスケールしないことが分かっていながら進むうち，やはりみんな使わなくなった．

楠：本当はあれってブロックチェーンも解になりそうな気もしたのですが，トラストレスと言っているからなのか，あまりこっちの用途には広がらなかったですね．

上原：そうですね．

崎村：まだちょっとその辺は頑張ってみたいなとか思っているのですけれども，その変形としてこの間，僕は自分の公開鍵を Twitter でツイートしたのですけれども（笑）．

上原：せっかく暗号技術も進んできたのだから，運用も UX もそんなにおかしくならない全体をデザインしたスマートな仕組みにしないと S/MIME の置き換えになるようなメッセージングは出てこないような気がしていて．それが進むまでは PPAP がなかなか打ち倒せるようなものにならない．でも PPAP というのは UX 的には最低なのにどうして死なないんだとは思っています（笑）．

崎村：いや，あれはコンプラで強制されるから．

楠：あのコンプラ村の人たちの UX への関心の低さって何なんでしょうね？

崎村：ユーザブル・セキュリティとか，ヒューマン・セントリック・セキュリティとかと対局にいる感じ．しかし，PPAP を強制する人たちって，本質的にセキュリティが分かってないんでしょうね．分かってたらあんなことしないはずだから．日本のローテーション人事の特質で，専門家を当てないというところにも問題があるかもしれない．だから日本だけで PPAP がはやるみたいな．

上原：1 つ確実に言えることは，ルールを決めて守らせる人が，エンジニアリングにも UX にも仕事の効率

を保つことにも興味がない．本来は，どうやって効率を上げるかを考えてもらわなければならないはずなのに．

崎村：科学的理由がないところでのドグマがあって，そのドグマによって強制される儀式を踏んでいれば，科学的に間違っていてもそれが正当化されてしまう．科学的に安全を求めるのではなく，儀式によって安心を求めているように思える．

楠：安全なものをくださいと言っても，完璧に安全なものなどない．それが認知的不協和を呼ぶ．セキュリティに金をかければかけるほど不安になる病．だから安心を求めにいく．

認証連携ファイルアクセス制御

崎村：認証連携ファイルアクセス制御は，アクセスを許す相手の属性（通常はメールアドレスなど）を指定して，当該ファイルへのアクセス制御を行う仕組みです．それでそのファイルへのリンクをメールやチャットなどで送る．これが海外で割とメインストリームになってきているのかなという気がします．

大泰司：今，PPAP の自動化ソリューションを使っている企業はこれを簡単に導入できるはず．オプション料金がかかるところと，そのまま標準についているところがありますけど．

楠：やはり私の原稿でも書きましたが，結局，添付ファイルをやめてリンクを送ればいいんじゃないかと．そうすれば，添付ファイルにアクセスするというか，送りたかったものにアクセスするタイミングでもう 1 回，認証認可も走るし，あとから取り消すこともできる．今，Office 365 も，G Suite も，大体そんな実装になってきている．添付ファイルではなく，クラウドなりでファイル共有サービスとの連携に寄せていけば，ストレージも余計に食わないし，メリットはでかい．

崎村：これが結構，実はメインストリームに今なってきている感じがしますよね．

クラウド共有

上原：ただ，そういうクラウドはだれか分からない管理者が見ているかしれないから信用しないというのは分からんでもない．その意味で面白いのは Firefox Send．クラウドに確かに保管されるのだが，まずアップロードのところで暗号化される．Firefox Send 管理者には中身は見えない．鍵は URL に含まれた状態で相手に送られる．相手がメールを開いて，Firefox Send のサーバにアクセスしにきた瞬間に鍵が届いて，解きながらダウンロードされる．すごくよくできているなと思うのです．

ただ，惜しむらくは，URL に鍵が含まれているので，最後の瞬間に鍵がサーバにいっている．あと一歩 end-to-end 暗号化に足りない．

ただ，よく考えたら，その Firefox Send を運営する立場からすると，自分のところにあるストレージは全部暗号化されているので，たとえば，それこそ捜査機関がやってきて，お前，出せと言われても，いや知りませんと言えるというのが一番の実はメリットなのではないかなと思いながらあれを見ていたのですね．

崎村：Firefox Send みたいなのはどのカテゴリですかね．

楠：あれはクラウド共有の一種類なのかな．end-to-end encryption までやっているとちょっと違いますけれどもね．Firefox Send，好きすぎて，会社用に立てましたよ（笑）．

上原：いや，会社用に自分で Firefox Send を立てるというのが一番安全でいいと思うのですよね．Firefox Send のもう 1 つの欠点は送信者の認証がないこと．メールが送信者認証されていればいいのですけれども．Firefox Send を自ドメインで運営すれば，少なくともその組織からきたというのが分かる．

楠：はい．

崎村：わたしは，Firefox Send じゃないけど，NextCloud を自分のドメインで立てて，そこからリンクを共有するとかやってます．結局この手のものとい

うのはあれですよね，送信者認証，受信者認証，メッセージ認証，この 3 つと，それに基づく認可に尽きるのですよね．

上原：そうですね．はい．

楠：それで今，Firefox Send をまず立ててみて，銀行の業務要件に従ってそういうファイル受け渡しツールとかをつくれたら PPAP の代わりに売れないかなとか検討したのですが（笑），結局 end-to-end encryption している瞬間，ウイルススキャンをかけるみたいな要件を満たせなくてつらいみたいな．

上原：いや，だから，Firefox Send の受け取り手順に 1 枚かませて，受信側組織はファイルをダウンロードしてウイルスチェックをしてからエンドユーザに渡すみたいなソリューションとセットでやればいいかと思っているのですよ．

楠：それはそういうサーバ立てて復号するのですよね．

上原:ええ．だからまあそういうのをちゃんと動かすサーバをつくらなければいけないんですけど．

楠：ああ，受ける側でそれをインターセプトしてというのはなんかだんだん何のために何をやりたいのかが分からなく．

上原：まあでも自分の組織の中で閉じてできるのなら，たとえばその受け取った Firefox Send の URL を社内のある Web Form に突っ込むと，sanitize してから送ってくれるみたいなソリューションでもいいと思っていて．

楠：受け手のソリューションを別に用意するという．

上原：そうそう．そうです．

楠：代わりにファイルをダウンロードして，無効化なり，アンチウイルスなり，チェックをかける．

上原：そうそう．それでそのあとメールでエンドユーザに送ったら元の木阿弥かもしれないので，たとえば，共有フォルダにぽこんとその人の権限で置いてくれみたいな．

楠：ではそういう Firefox Send に Selenium かなんかでアクセスをして，ひと通りのことをやってくれるやつを端末側で用意をしてやる．

上原：そうです．はい．

楠：なるほどな．なんかそこまで立てるのだったら，もうちょっと素敵なプロトコルにしたくなるな（笑）．

上原：まあそれはそうですね．はい．

組織超えグループウェア

楠：でも Firefox Send って，若干関心が高まったのというのはやはりみんな宅ふぁいる便難民になったときだと思うのですけれども．あの宅ふぁいる便がリスク管理部門をクリアしていたというのは一体何だったのかなと．

大泰司：あとなくなってしまったのですけれども，サイボウズ Live を使っている時期がありましたね．会社をまたいでグループをつくるとき，よく使われていましたね．

上原：組織越えのグループウェアみたいなものですよね．

崎村：そうそう．

大泰司：今，その人たちはだいたい Slack にいったんですよね．でも，Slack に移れないおじさんが結構，残ってしまいました（笑）．そういう人たちはいま Facebook に流れ込んでいる．

楠：でも，メッセンジャーでは置き換えにならない．業務で使うのだったら，どちらかと言うと Slack などのビジネスチャットなのかなと．

上原：システム管理部門にすごく力があれば，一番いい逃げ先は今，Teams だと思う．だけど，テナントデザインがすごい難しい．

楠：それは Active Directory の運用の細かいところが．

上原：いや，そもそもチームをつくるという権限をだれに与えるかとかですね．あと，チームでつくると，グループウェアとしてファイル共有ができたりするのですが，その仕組みが，あの上にあるのですよ，何だっけ．

楠：SharePoint.

上原：SharePoint の上にあるのですよ．その連携が，いろいろ気持ち悪いのですよね．

楠：SharePoint をパーツっぽく使っているおかげで，

Teams でごにょごにょやっているといつの間にか SharePoint 側に不思議な枝が生えていきますよね.

上原：そうそうそう．不思議なファイルが SharePoint にできるのですよね．それもなんか気色悪くて.

楠：しかもそれもみんな検索の対象とかにいつの間にかなっている.

上原：そうそうそう．それで，ある大学の先生から聞いてびっくりしたのですが, Teams でフォルダを掘るときに, 最初, 適当な名前で付けておいて, あとでちゃんとした名前に変えても, SharePoint にできるフォルダが，その最初の名前のまま（笑）.

楠：リソース名だけ変わる.

上原:リソース名だけ変わるので（笑），最初「ほげほげ」で作ると，「ほげほげ」というフォルダが SharePoint 側にできて，ずっとそのまま（笑），ひどいシステムだということが分かった.

楠：なかなか切ないものがありますね.

上原：びっくりしましたね.

大泰司：だから今そんな感じでプロジェクトごとに使うツールが別々でものすごい大変.

ビジネスチャット

楠：それで言うと，我々はもはや電子メールではなくて LINE とか，Telegram とか，素晴らしい end-to-end encryption ソリューションを持っているわけで，メールが残っているのは法人の問題ですよね．業務で使えるのだったら，どちらかと言うと，Slack とか，ビジネスチャット系なのかなというふうに.

上原：まあ電子メールがいいのはインターオペラビリティがちゃんと確保されていること．あと，これはもう文化の問題ですが，仕事の依頼を LINE で送るとは何事だと怒り出す人がいる（笑）.

崎村：昔はメールだって怒られたのですけれどもね.

上原：そうそうそう（笑）.

大泰司：昔ね，メールで怒られていましたよ（笑）.

上原:今はメールも，マナーと流儀と仁義を切ればちゃんと認められるようになった．だからインスタントメッセージングでも，インターオペラビリティあるかたちで標準のものが出てきてくれればいいのですが，ちょっと望み薄なので，しばらくはメールの地位は揺るがないという気はしているのですよね.

楠:そうなのでしょうね，XMPP（Extensible Messaging and Presence Protocol）とか，一時期，インスタントメッセージングプロトコルの標準化の議論もだいぶあって，iMessage などオープンな仕組みにつながったりしましたが，あまり流行らなかったですね.

上原：結局，まだまだメッセージングの世界は囲い込みをしないことには競えないのですよね，きっと.

楠：あとは結局，ことごとく UX にかかわるものが規格に響いてきてしまうから，標準に乗った瞬間に中途半端なものしか出せないというのはある気がしますね.

上原：なるほどね．それはそうですね.

楠：やはり鍵のハンドリングというのは，最後，一番，プロプラで残りそうな部分というか, PKIX WG（PKI の標準化を議論する IETF のワーキンググループ）がうまくいかなかったことによって，オープンでやってうまくいった動きはあまり少ない.

業務システム

大泰司：電子契約というのはここ 1 ～ 2 年でどんどん入ってきている．調達や営業部門では，見積書が PPAP できて，イラッとするところですが．でも，これはもう電子契約にどんどん移っていきますね.

崎村：定型業務は電子契約や CRM（Customer Relationship Management）にどんどん移っていくという話ですね.

楠:そう，寄せていくのが大事．ツールがないところだと，添付ファイルのようななんでも送れる仕組みを使って，その結果問題を起こしたりする．要りもしない実行ファイルとかも送れるようになっていて.

上原先生ともよく話しているのですが，電話にしても，メールにしても，好きに入力した文字列で指定した相手に自由にものを送れる仕組みはやはり限界

がある．社内コミュニケーションなど密度の高いやりとりは，Slack や Teams など，決まった相手とのやりとりに限定したものに寄せていく．それで電子メールの使い道をできるだけ日々の業務から減らしていく．大代表のメールに入れると，セールスフォースで CRM で反応するみたいな，汎用メーラーを使わないようにしていくのが本当はいいのだろうなと．

上原：そうですね．

崎村：だから業務で，いわゆる電子メールを使うのは本来間違っていると思うのですね．これは金融機関のコンサルをやっていたときにも強く言って，ネットワークの分離などではなく，本来は顧客向けのメールだったらちゃんと CRM から出せと．そうすると文面のコンプライアンスも何もかも全部入るわけですよね．EUC (End User Computing) をやるなと．電子メールなんていうのは EUC の最たるものだろうと．

楠：しかもメールボックスというのは個人単位なので，人事異動があったときに管理できなくなる．社外とのやりとりは全部 CRM でいいんじゃないかなと．

上原：メールがいろんなものの非効率を生んでいる．組織内でも添付ファイルをつくって，ご査収くださいとかいうのを組織内でぐるぐる回しながら，いろんなバージョンのファイルが散逸していく．リスクも増えていくし，バージョン管理もできない．あの状況を何とかしないといけないという意味でも，メールはもうなくしてしまったほうがいいと思っていますね．

大泰司：オンラインストレージを使うのがいいと思います．現実にもうかなりそうなっている．PPAP の誤送信防止ソリューションのベンダも，大手は設定 1 つでオンラインストレージを使うようになっている．

楠：なんか明らかに異なる文化圏があって，VDI (Virtual Desktop Infrastructure) が入っていて，フィルタリングソフトで主要なクラウドサービスはみんなフィルタリングしている一連の会社や役所がある．あの文化圏の人たちは，在宅勤務のサポートに苦慮しているような感じになっていますが，これからどうするのでしょうかね．

より良い方式のまとめ

崎村：大体，出揃いました．議論に出た「より良い方式」をまとめますと，まず第 1 に，できるだけ通常のメールを使うのはやめる．通常の業務は汎用メールクライアントを使うのではなく，CRM，EDI (Electronic Data Interchange)，電子契約システムなどの業務システムを使って行う．これらが SMTP を使う場合には TLS を強制する．

非定形のコミュニケーションは，お互いに認証されている Slack や Teams などの「ビジネスチャット」を使う．ファイルはこの上で送るか，「認証連携ファイルアクセス制御」の効いているクラウドストレージを使う．そんなところでしょうか．

楠：この辺に落ち着く気しかしないですね．

日時：2020 年 4 月 24 日
場所：オンラインにて

■**崎村夏彦（正会員）** nat@nat.consulting

本会 SC 27/WG 5 主査．OpenID Foundation 理事長．ディジタル・アイデンティティとプライバシに関する国際標準化が専門．著した規格に OpenID Connect, JWS, JWT など．

■**大泰司章** otaishi@gmail.com

三菱電機，日本電子計算，JIPDEC を経て，PPAP 総研設立．電子契約，電子署名，メールや Web のなりすまし対策を普及．PPAP やハンコ等の非効率な取引慣行を変えて，真の働き方改革を目指す IT コンサルとして活動中．

■**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．

■**上原哲太郎（正会員）** t-uehara@fc.ritsumei.ac.jp

和歌山大学，京都大学，総務省を経て 2013 年より立命館大学情報理工学部教授．専門はサイバーセキュリティ，システム管理，ディジタル・フォレンジック．入力しにくいだけの Excel 帳票や無駄な押印の撲滅にも興味を持つ．

■表 -1　PPAP に代わる安全な方式

項番	方式名	方式説明	メモ	経路安全性	到達先安全性	誤送信耐性（受信者認証）	送信者認証	マルウェアチェック	デメリット
				送信から受信までの経路上で盗み見られることに対処してあること.	到達先のメールボックスをマルウェアが見ていても読み取れないようにすること.	意図した送付先以外は読み取れないようにすること.	受信者が，そのメッセージが誰から送信されたかが分かること.		
1	SMTPS の強制	SMTP MTA Strict Transport Security (MTA-STS) https://www.rfc-editor.org/info/rfc8461 DNS を用いてドメインが SMTPS を強制してるかどうかを宣言.		○ TLS による.	× 到達先安全性は守れない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	× 送信者認証は含まれない.	○	?
2	事前鍵交換共通鍵暗号化ファイル添付	A と B がファイルを交換するときに，あらかじめオフラインで共通鍵を交換しておいて，以後，その鍵でファイルを暗号化してメールに添付する.	本来の PPAP のあり方．鍵は十分に長くないといけない．鍵の管理と利用には 1Password のような企業モードがあり複数で鍵を共有できるパスワード管理ソフトを使うしかない.	△ 暗号化強度はパスワード強度に依存する.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	○ ファイルの暗号化と送信先の指定が合致しなければ読むことはできない.	○ パスワードが安全に管理されていれば送信者認証が可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	鍵をプロジェクトごとに覚えるのは困難.
3	公開鍵暗号化ファイル添付（PGP など）	A と B がそれぞれの公開鍵を一定の場所に公開しておき，その公開鍵を使ってファイルを暗号化してメールなどに添付する.	メール以外でも使える．キーサーバがスケールしない．受け取り手の端末にソフトがインストールされていないのがネック．エストニアでは全国民に当該ソフトを配布，国民 ID カードを使って処理できるようになっている.	○ 暗号強度は暗号方式に依存.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	○ ファイルの暗号化と送信先の指定が合致しなければ読むことはできない.	○ 送信者認証が可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	ソフトが普及していない.
4	公開鍵メッセージ暗号化（S/MIME）	PKI の個人証明書をベースに MUA で公開鍵で暗号化・署名する.		○ 暗号強度は暗号方式に依存.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	○ 署名をつければ可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	エンドユーザが使えないと，サポートコストが上がってしまう.
5	DNS を使った ID ベース暗号	ID ベース暗号を用いた実用的電子メールシステムの設計と実装（2019-IOT-044）. http://id.nii.ac.jp/1001/00194748/	DNS が信頼できるのであればこれに頼った鍵配布ができるのではという考え方.	△ DNS になりすましの危険がある．ただし可能性は低い?	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	○送信者認証が可能.	秘密鍵を送信側・受信側の MTA で管理する運用を想定．その場合 MTA でマルウェアチェックできる.	まだ標準化されていない.
7	認証連携ファイルアクセス制御	アクセスを許す相手の属性を指定して，当該ファイルへのアクセス制御を行う（ABAC）．そのファイルへのリンクをメールやチャットなどで送る.	現在のメインストリームになってきている．PPAP ソリューションには実はすでにオプションとしてあるものが多い.	○ TLS による.	サーバ上のファイルを自動で読まれることは，認証がしっかりしていればない．また，いつ誰によって読まれたかのログを取ることもできる．ダウンロード後は End Point Security のレベルによる.	△ アクセス制御がかかるため，誤送信しても読めないようにすることは可能.	△送信者が自ドメインでサーバを立てればある程度可能．リンクの送信にビジネスチャットなどを利用すれば可能.	マルウェア配布サイトかどうかは，URL のレピュテーションである程度管理可能．これに，エンドポイント検知を組み合わせる.	クラウド事業者のサーバを使うと，クラウド事業者の管理者や監督する国の政府にに読まれてしまうのではないかという心配がある.
8	クラウド暗号化ファイル共有	暗号化したファイルをクラウドに置き，それを解く鍵と URL を相手に送る．受信者が URL にアクセスすると，復号化されてダウンロードされる（例：Firefox Send）.	会社用に自分で Firefox Send を立てるのが，一番安全でよいのではないか.	○ TLS による.	× マルウェアがパスワード付きリンクを読めるとファイルも読めてしまう.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	△送信者が自ドメインでサーバを立てればある程度可能．リンクの送信にビジネスチャットなどを利用すれば可能.	マルウェア配布サイトかどうかは，URL のレピュテーションである程度管理可能．これに，エンドポイント検知を組み合わせる.	パスワード付きリンクを読めるとファイルも読めてしまう.
9	組織超えグループウェア	サイボウズ Live などを，他組織の人とも使う方式.	今なら Teams など.	○ TLS による.	適用される認証強度による.	△ 登録したユーザのみに送れる．ただし，間違った部屋に送ることはあり得る．その場合も削除可能.	○ 登録したユーザのみが使える.	エンドポイントで検知	グループウェアにおけるアカウント作成・招待が手間.
10	ビジネスチャットにおける添付ファイル	Slack や Teams など.		○ TLS による.	適用される認証強度による.	△ 登録したユーザのみに送れる．ただし，間違った部屋に送ることはあり得る．その場合も削除可能.	○ 登録したユーザのみが使える.	エンドポイントで検知	グループウェアにおけるアカウント作成・招待が手間.
11	業務システム	電子契約，ERP，CRM などを使う方式.	定型業務は，業務システムに寄せていく．社外とのやりとりは，本来は業務システムを通じて行うべきで，メールソフトのような End-User-Computing はやめるべき.	○ TLS による.	受信者のシステムによる.	○ 業務内容に応じて送信先が自動的に選ばれる.	△ 業務システムが利用するプロトコルによる．電子署名をつけるなどすれば，送信者認証は可能.	△業務システムが利用するプロトコルによる.	定型業務のシステム化が必要