【講演レポート】JIPDECセミナー
パネルディスカッション「これからのなりすましメール対策」

モデレーター　PPAP総研　大泰司　章　氏
パネリスト　フィッシング対策協議会 証明書普及促進WG　主査
（サイバートラスト株式会社）　田上　利博 氏
フィッシング対策協議会 証明書普及促進WG　副主査
（GMOグローバルサイン株式会社）　稲葉　厚志 氏
九電ビジネスソリューションズ株式会社　ビジネスソリューション事業部
ビジネスソリューション第2部　部長　渡辺　雅久 氏
一般財団法人日本情報経済社会推進協会　セキュリティマネジメント推進室
主査　高倉　万記子

●JIPDECのS/MIMEへの取組み（大泰司　章氏）

JIPDECはS/MIMEの普及にあたり、これまで「S/MIMEシンポジウム」の開催や、S/MIMEに利用可能なパブリック電子証明書の利用状況調査の実施、インストールガイドの発行などを行ってきました。
しかし、S/MIMEそのものが知られていないということから、「エスマいぬ、ディーキぃぬ」といったキャラクターを誕生させ、シールや、LINEスタンプなどで普及を行っています。

本日は、なりすまし対策に関する最新状況の共有ということで、フィッシング対策協議会の普及活動、国際的標準化団体「CAブラウザフォーラム」の動向、S/MIME事例紹介、JIPDECが行っているなりすまし関連の調査結果についてご紹介いただきます。

●S/MIMEの普及啓発における活動について（田上　利博氏）

フィッシング対策協議会　証明書普及促進WGは、ウェブサイトの真正性・実在性の普及啓発を目的に発足しました。国内調査では常時SSL対応しているサイトが約87%となっています。電子証明書の活用は身元証明と実在証明に有効であり、本日のテーマであるS/MIME署名がフィッシング対策に有効と考えられています。

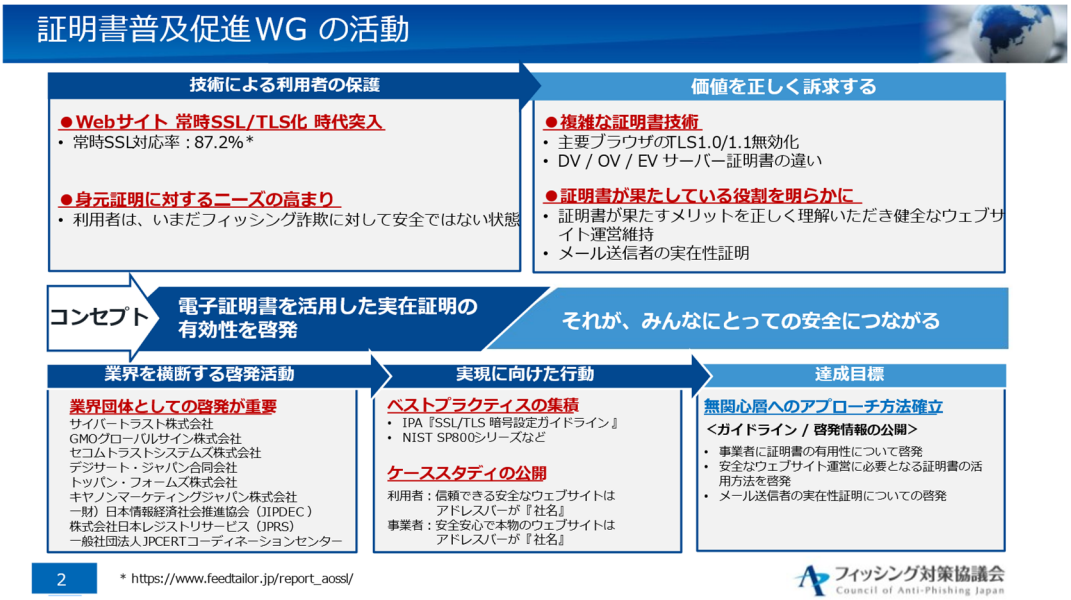
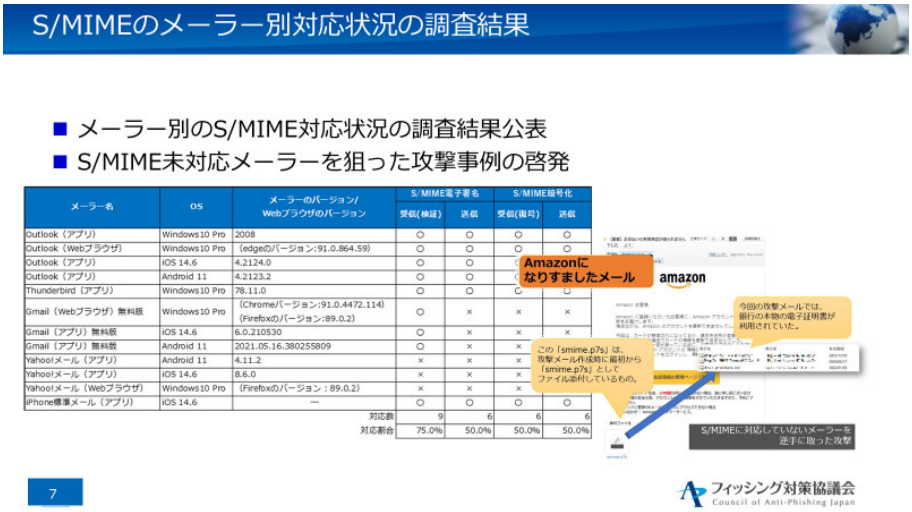


図1. フィッシング対策協議会　証明書普及促進ＷＧの活動内容

当WGでは、フィッシング対策についてBtoB、BtoCへのサービス提供における事業者の高い信頼性を担保することが重要であり、技術面での公開鍵暗号方式の電子証明書の普及促進を考え、協議を重ねています。
メール送信者の実在性証明の普及啓発が当WGのミッションであり、Chrome、Edgeなどさまざまなブラウザごとのサーバー証明書の表示の違いなどをコンテンツとして紹介しています。事業者向け啓発活動として、3種類のサーバー証明書のユースケース情報も公開しています。

「S/MIME」については、JIPDECと連携してS/MIMEのメーラー別対応状況の調査結果※1を公開しています。
フィッシング対策ガイドラインでは、要件として、利用者が正規メールかフィッシングメールかを判別できる対策として、事業者が対応していることをホームページで公表することが必要であると明記しています。

今後の活動としては、事業者および利用者向けにS/MIME署名に関して、このメールが安全か否かを理解してもらえるような啓発活動を行う必要があると考えています。さらにDMARCとS/MIMEの違い、業界内では「DMARCだけでよい」との一部意見もありますが、それぞれの利用用途、メリット／デメリットを啓発・コンテンツを提供していきたいと思っています。
今後も、S/MIMEのメーラー別対応状況の調査や、S/MIME未対応メーラーを狙った攻撃事例の啓発も行っていきたいと思います。



メーラー名	OS	メーラーのバージョン/Webブラウザのバージョン	S/MIME電子署名 受信(検証)	S/MIME電子署名 送信	S/MIME暗号化 受信(復号)	S/MIME暗号化 送信
Outlook（アプリ）	Windows10 Pro	2008	○	○	○	○
Outlook（Webブラウザ）	Windows10 Pro	（edgeのバージョン:91.0.864.59）	○	○	○	○
Outlook（アプリ）	iOS 14.6	4.2124.0	○	○	○	○
Outlook（アプリ）	Android 11	4.2123.2	○	○	○	○
Thunderbird（アプリ）	Windows10 Pro	78.11.0	○	○	○	○
Gmail（Webブラウザ）無料版	Windows10 Pro	（Chromeバージョン:91.0.4472.114）（Firefoxのバージョン:89.0.2）	○	×	×	×
Gmail（アプリ）無料版	iOS 14.6	6.0.210530	○	×	×	×
Gmail（アプリ）無料版	Android 11	2021.05.16.380255809	○	×	×	×
Yahoo!メール（アプリ）	Android 11	4.11.2	×	×	×	×
Yahoo!メール（アプリ）	iOS 14.6	8.6.0	×	×	×	×
Yahoo!メール（Webブラウザ）	Windows10 Pro	（Firefoxのバージョン：89.0.2）	×	×	×	×
iPhone標準メール（アプリ）	iOS 14.6	—	○	○	○	○
		対応数	9	6	6	6
		対応割合	75.0%	50.0%	50.0%	50.0%

図2. S/MIMEのメーラー別対応状況の調査結果（2021年9月発表）

※1 https://www.jipdec.or.jp/topics/news/20210928.html

●「CA/BrowserフォーラムのS/MIME Certificate Working GroupにおけるS/MIME用電子証明書の標準化動向について」（稲葉　厚志氏）

CA/Browserフォーラムは当初SSL/TLSサーバー証明書の改良を目的として設立されたフォーラムです。電子認証サービス事業者（認証局）、製品ベンダー（ブラウザベンダー）、監査機関を主なメンバーとして構成されており、フォーラムでは、SSL/TLS証明書発行時の認証プロセスを厳格化したEVSSL/TLS証明書のためのガイドラインを始め、さまざまなガイドライン・要件の作成を進めています。

フォーラム内にはいくつかWGがありますが、今回のテーマであるS/MIME Certificate WGは2020年6月に設立が承認され、翌月から活動を開始しています。フォーラムの意思決定は、メンバーから提起されたテーマについてメンバー間で議論を重ね、合意形成を諮りつつ、最終的に投票による議決・承認および知的財産権の確認期間を経て最終決定され、WG新設やガイドラインへの反映等が行われます。また、フォーラムの一般向けウェブサイトでは意思決定に関わる議論や投票結果、ミーティング（オンラインおよびFace-to-Face）議事録、ガイドライン、要件ドキュメント等、さまざまな情報を公開しています。S/MIME Certificate WGでもミーティング議事録を公開しており、サイトを閲覧いただくことでWGでの議論や検討の状況を把握することができます。S/MIME証明書WGのメンバーは、アメリカ、ヨーロッパ、アジアといった各地域でビジネスを展開している認証局やグローバルにビジネスを展開している認証局、そしてApple、Google、Microsoft、Mozillaなどのブラウザベンダー（メールアプリケーションも持つ）およびWebtrust、ETSI監査に係るコミュニティからのタスクフォースメンバー等が参画しています。
WGでは、eメールアドレス管理状況の確認、鍵管理および証明書ライフサイクル、S/MIME用電子証明書およびそれを発行する認証局証明書の証明書プロファイル、認証局運用規定、物理的／論理的セキュリティ、S/MIME用電子証明書に記載される自然人および法人の身元確認など、S/MIME用電子証明書

としての特徴的な項目およびSSL/TLSサーバー証明書やコード署名用証明書を発行する認証局として共通的な項目を認識し、かつ既存のスタンダードやガイドライン等も参照しながら要件の検討を進めています。
そして、目標とする主要成果物としてはS/MIME用電子証明書に係る要件をまとめたドキュメントとして、”Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates”の作成と公開を目指しています。
”Baseline Requirements“は基本的には準拠が必須の要件として作成しますが、主要なブラウザベンダーがフォーラムに参加して作成されるSSL/TLSサーバー証明書のBaseline Requirementsとは異なり、フォーラムに参加していない多くのメールアプリケーションベンダーが存在する状況下においては、より多くのメールアプリケーションベンダーに受け入れられて、準拠が求められるまでは、認証局に対してS/MIMEのBaseline Requirements準拠の必須化を求めないこととWGのCharter（WG設立趣意書）では規定しています。ただ、S/MIME対応メールアプリケーションを持つブラウザベンダーが規定する認証局ルート証明書搭載要件の中に、Baseline Requirementsに規定されている／いないに関わらず、S/MIME用電子証明書に関する要件が規定されてしまうと、規定を守らない認証局のルート証明書は外され、その認証局の発行するSSL/TLSサーバー証明書、コード署名用証明書、S/MIME用電子証明書といったあらゆる電子証明書が当該ブラウザベンダー製品上で正しい電子証明書として認識されなくなり、認証局としてのビジネスが立ち行かなくなるため、結局のところブラウザベンダーからのルート証明書搭載要件について認証局は何が何でも準拠が必須となってしまう現状もあります。

参考）活動トピックス

図3. S/MIME Certificate WGの活動トピックス

【大泰司】日本ではあまり話題になりませんが、海外では盛り上がっているのでしょうか？

【稲葉】今盛り上がっているかと問われると、各国の事情もあり、盛り上がっているとは必ずしも言い切れないかと思いますが、CA/Browser ForumでWGが立ち上がりBaseline Requirements作成に向けて動き出したということは、今後に向けてその必要性が認知されていく方向なのではと期待します。WGではS/MIME証明書を署名用証明書と暗号用証明書に分けてはどうか、S/MIME単一目的とアクセスコントロールや文書・データへの電子署名等と合わせ、複数目的で使うにはリスクの高まりが異なるのではないか、などの議論もしています。エンドユーザが自分の秘密鍵と証明書をローカルで管理するパターンと、自分の秘密鍵も含めてベンダーに預けてしまうリモート署名の場合にどのような要件が必要か、など、アメリカ・ヨーロッパ・アジアの認証局メンバーを中心に、各国・各地域事情を背景としたさまざまな議論も上がるので、落としどころを見出すのが困難な局面も考えられますが、何とかしてドラフトBaseline Requirementsについて今年の内には、ある程度の形にすることを目指してWG作業を進めています。

●［S/MIME導入事例紹介］

九州電力グループのS/MIME導入事例、運用自動化を実現した仕組み『CertCONNECT（サートコネクト）』でS/MIMEをビジネスメールのマナーに」（渡辺　雅久氏）

九州電力グループは、グループウェアのメールソフトを改修し、「社内メール」と表示させることにより「社外メール」との区別を行っていましたが、Office365への切替えにより、その区別がつけられなくなりました。社外メールの開封への注意喚起・標的型攻撃メール訓練など、周知徹底等を行ってきましたが、よりわかりやすくするためS/MIMEの導入を検討しました。
OutlookはS/MIME対応ソフトであり、本人発信の証明がつくことで非常にわかりやすかったのですが、一方で、九電グループ社員他1万人超、2万台近くのPCを対象に、電子証明書のインストール用パスワードの厳格な管理、証明書発行・管理プロセスそのものの管理など、運用面での課題が多く発生しました。
そこで、さまざまな課題を整理しつつ、S/MIME導入の自動化の仕組みを作り、2019年6月に九電グループでの完全自動化が完了しました。

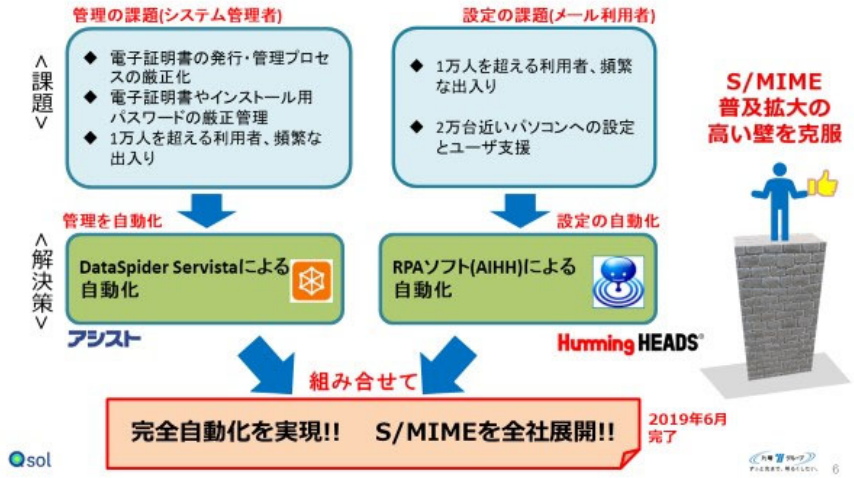


図4. S/MIME導入上の課題と解決策

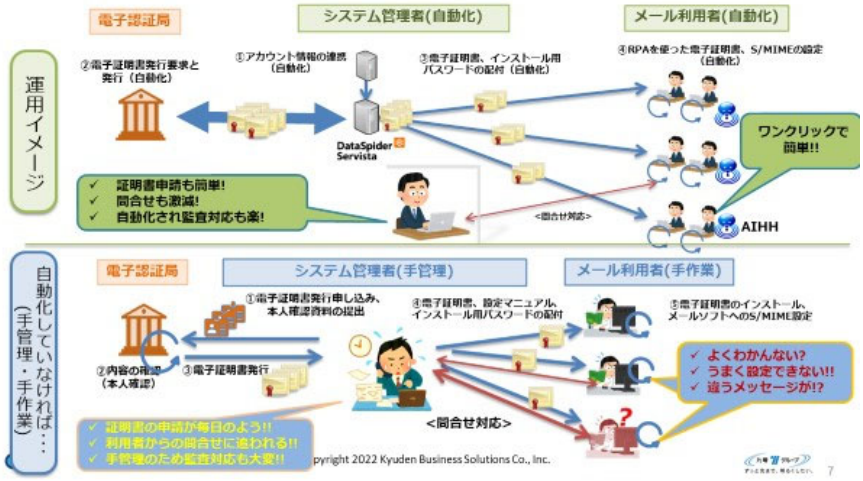


図5. S/MIME自動化運用イメージ

この仕組みはJIPDECを含め関係4社で共同特許を取得しており、現在、九電ビジネスソリューションズ（QBS）が「CertCONNECT（サートコネクト）」として、企業にサービスを提供しています。

運用の実態として、利用者は電子証明書の更新時にワンクリックするだけで、電子証明書付きのメールを送信でき、運用負担もない状況です。一方、システム管理者側では導入当初、文字化けや、一部の自治体で無害化ソリューションにより電子署名が外れてしまうなどがありました。現在は運用負担は少ない状況です。

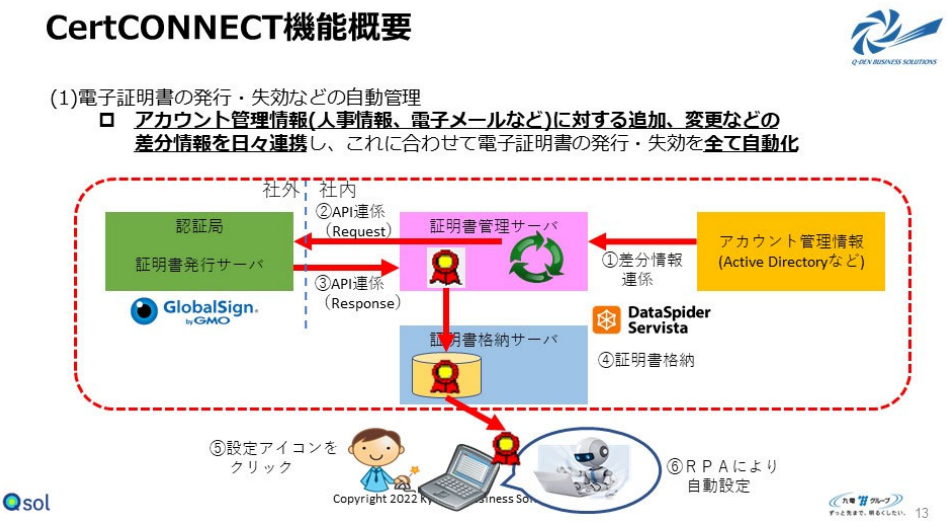
S/MIME化率は約6～7割です。送受信全体の6～7割は社内、グループ会社間のやり取りとなりますが、残りの3割は外部からのメール受信です。メルマガや営業メールの受信件数も多く、MicrosoftのTeams等も活用していますが、メールの利用自体がなくならないので、その対処も必要です。

また、社外へのPRが重要であることから、メール本文内に電子署名を付与している旨を記載するよう準備していますが、やはり皆様にもっとS/MIMEを認知いただき、ご利用いただきたいと願っています。

コロナ禍、DX推進等で必要不可欠なビジネスインフラとして、電子メールの活用はますます増えていく一方で、Emotetの復活やなりすましメールがなくならないことから、なりすましメール対策は今後さらに重要になると考えています。

SPF、DKIM、DMARCといったなりすまし対策に加え、受信者がなりすましメールではないことを可視化できるS/MIMEはますます重要になり、ビジネスメールのマナーになっていけばよい。さらにCertCONNECTなどのサービスを利用したS/MIMEの導入により、社内、取引先、顧客の安心・安全につながっていけばよいと思います。

参考）CertCONNECT機能概要



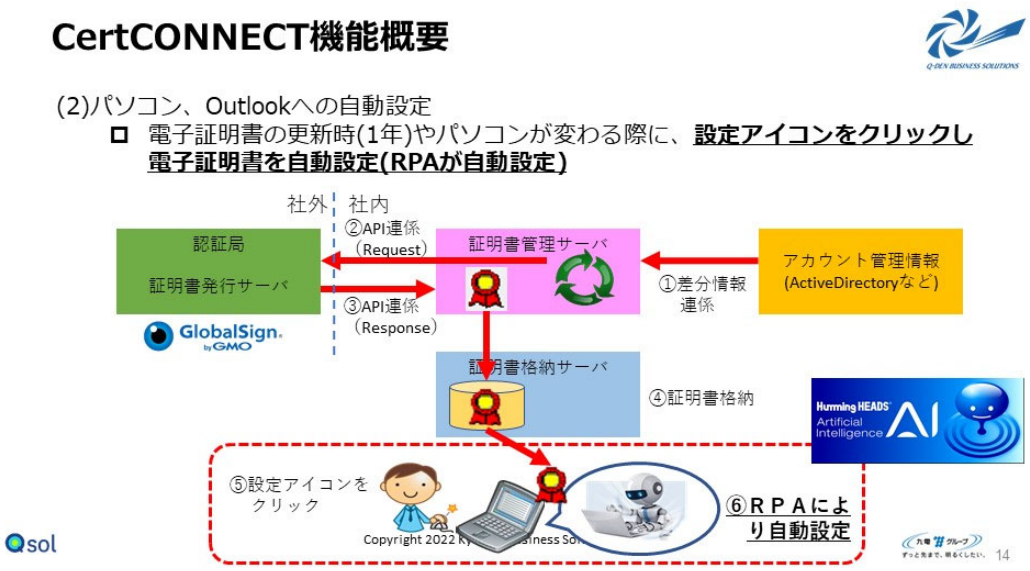


図6．CertCONNECTの機能概要

【大泰司】佐々木先生がS/MIMEについて解決すべき課題がある、と言われていましたが、解決できている点もあるのではないでしょうか？

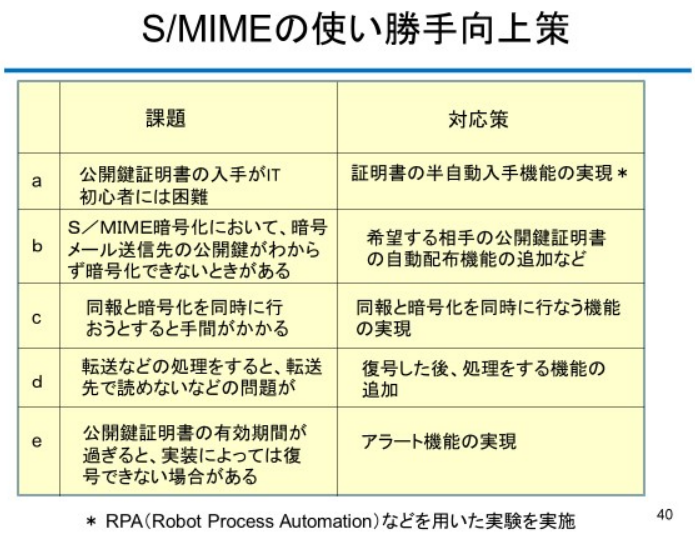


図7．S/MIME導入の課題（佐々木良一先生講演資料から）

【渡辺】 佐々木先生が挙げられた課題のうち、「a．公開鍵の入手困難」については、CertCONNECTは自動連係しているので、面倒ではありません。

「b．S/MIMEの暗号化ができない」点については、Outlookではボタン押下で暗号化できますが、送り先側での鍵の管理、暗号化した古いメールの複合化の運用などの課題も多いことから、当社は行ってい

ません。また、署名なしのメールの送信はできない仕組みですが、緊急避難的に署名なしのメールが送れるような機能も用意しているので、システム管理者がS/MIME署名管理上、特別な負担はありません。

●国の行政機関が発行するメールマガジンのなりすまし対策状況の調査結果（高倉　万記子）

なりすましメール対策技術として、S/MIME、SPF、DKIM、DMARCがあります。DMARCは米・英政府が導入しており、迷惑メール削減に貢献しています。JIPDECはこれらの技術普及のため、これまでさまざまなりすまし対策状況について調査を実施しています。

2018年2月には企業のなりすましメール対策の現状把握※2、2020年10月には自治体防災メールのなりすまし対策※3、2021年12月には国の行政機関、省庁が配信しているメルマガのなりすまし対策※4について調査を行いました。（各調査の詳細は資料参照）

■企業のなりすましメール対策調査

10万社を対象にSPF、DMARCの設定状況について調査を行いました。

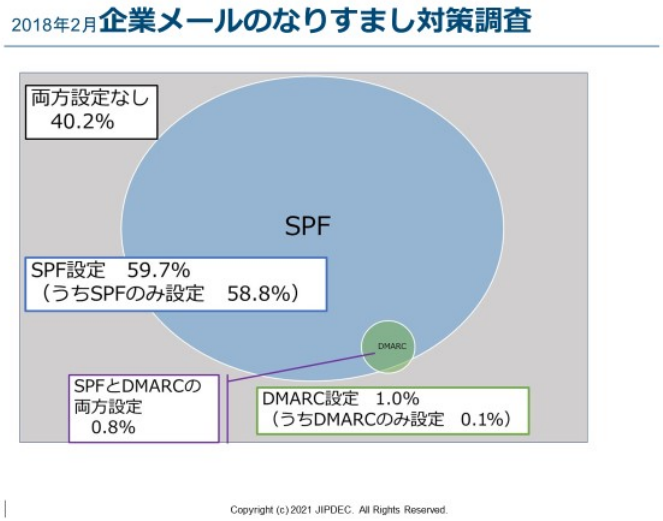


図8. 企業メールのなりすまし対策調査（SPF,DMARCの設定状況）

■自治体防災メールのなりすまし対策調査

都道府県、市区町村で防災メールを配信している1,122自治体のうち、配信メールアドレスが確認できた1,026自治体を対象に、SPF、DMARCの設定状況を調査しました。

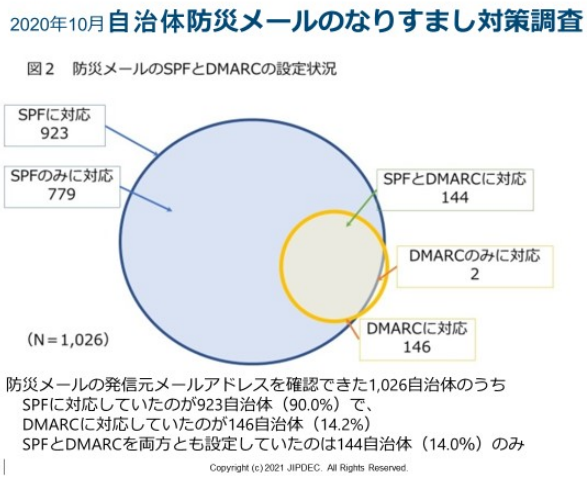


図9．自治体防災メールのなりすまし対策調査（SPF,DMARCの設定状況）

■国の行政機関、省庁が配信しているメルマガのなりすまし対策

国の行政機関、省庁が配信しているメルマガから実際に受信確認できた72件を対象に、S/MIME、SPF、DKIM、DMARCの設定組合せ状況について調べました。

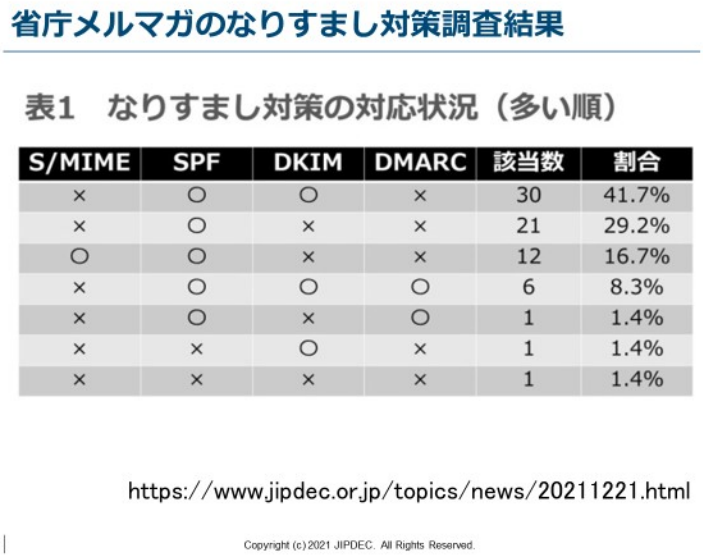


図10．省庁メルマガのなりすまし対策調査（S/MIME、SPF、DKIM、DMARCの組合せ状況）

JIPDECもS/MIMEを利用しています。NTTテクノクロス社のCyber Craft/Mailというソリューションを利用しており、協会から発信するすべてのメールにS/MIMEが付与されるとともに、誤送信防止機能により、外部へのメール発信の都度、宛先、文面、添付ファイルの確認が求められます。

（調査結果リリース）

※2　https://www.jipdec.or.jp/topics/news/20181211.html

※3　https://www.jipdec.or.jp/topics/news/20201020.html

※4　https://www.jipdec.or.jp/topics/news/20211221.html

【大泰司】興味深い調査結果です。SPFとDKIMを設定している割合は高いのに、DMARCは設定されていないのですね。
【高倉】DMARCは割と最近のものなので知られていないからだと思います。
JIPDECサイトで各種資料を公開していますが、さまざまな業種調査なども今後行っていきたいと思います。ぜひ、こんな調査結果がほしい、などリクエストがあれば、ご提示ください。

●パネルディスカッション「これからのなりすましメール対策」
参加登録時のアンケート結果および質問内容をもとにディスカッションを行いました。

（1）S/MIMEの設定状況

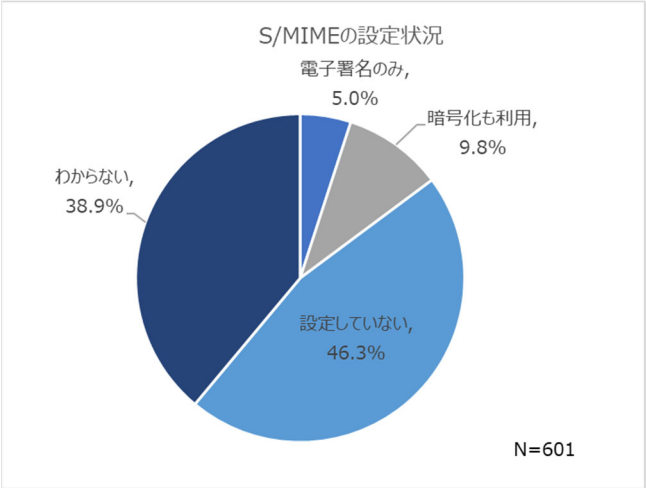


図11.　S/MIMEの設定状況

【田上】S/MIMEの設定状況について、「設定していない」「わからない」が多いようですが、S/MIME自体はわかっているが社内事情で設定していないのか、S/MIME自体がわからないというケースなどが含まれているのではないでしょうか。
【大泰司】本セミナーのテーマ自体「S/MIME」「PPAP」なので、S/MIMEについては理解されている方が参加されていると思います。
【田上】S/MIMEの場合、運用コストや管理、更新・失効などの手間もあると思います。企業が取り組みやすくなればもっと利用されるのではないでしょうか。電子証明書の配付や管理が重要だと思います。
【大泰司】九州電力の事例のように、端末への配布を簡単にして、運用をいかに楽にするか、またはゲートウェイで強制的に証明書を付けるか、2つの方法があると思います。
【田上】メルマガなどのメール配信サービスを使っている場合、S/MIME署名対応が進んでいけばいいと思います。
【大泰司】シェアの高いサービスでは電子署名対応しているなどがあります。署名を付けることで遅くなる、という点もあります。JIPDECの調査で防災メールに技術があまり使われていないという結果が先ほど紹介されました。

【田上】一斉同報の場合、S/MIME署名を付けることでトランザクションが遅くなってしまうことから、防災メールのように早急に配信されなければならないメールにはそぐわない、一般的な企業のメルマガであれば、証明書が利用されるのではないでしょうか。

（2）SPF／DKIM／DMARCの設定状況

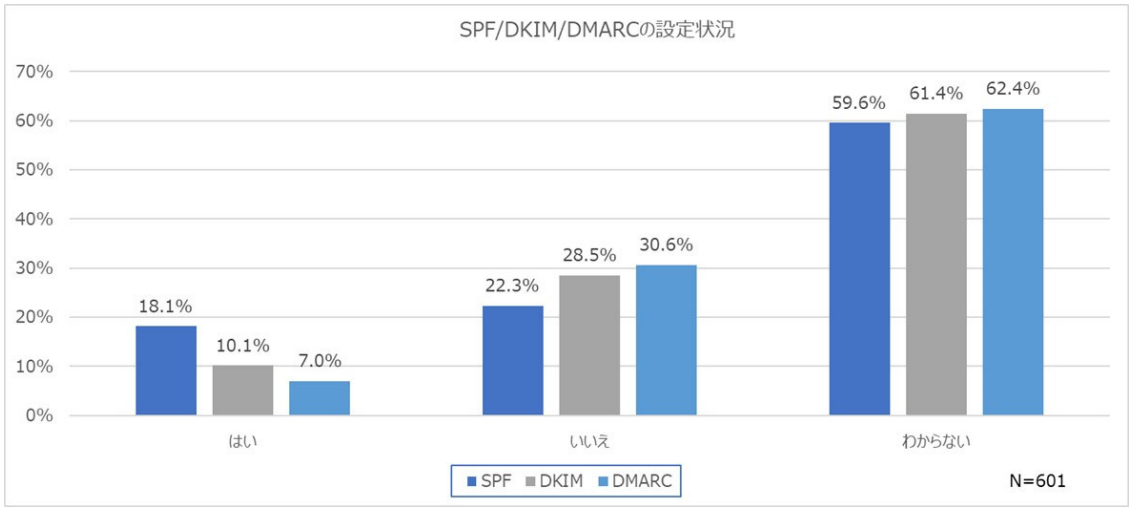


図12.　SPF／DKIM／DMARCの設定状況

【高倉】「設定していない」「わからない」の割合が高いのですが、これはおそらく自社の設定状況を把握していない回答者が多かったのだと思います。
【大泰司】設定状況については、ユーザ自身が気にすることではなく、会社の管理部門がわかっていればよいことです。それよりも受信側が署名の有無を確認できなければ、なりすまし対策になりません。たとえばOutlookでリボンが表示されるように、受信側で署名がついているか、わかるようになってもらいたいです。

（3）仕事でメインにつかっているメーラーの種類

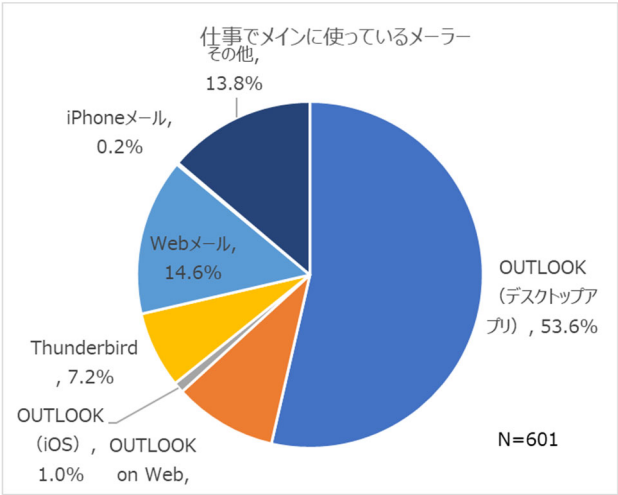


図13.　仕事でメインに使っているメーラーの種類

【渡辺】Microsoft社によると、大企業でのOutlookの利用率は高いそうです。CertCONNECTはOutlookのデスクトップを前提にロボティック・プロセス・オートメーション（RPA）が動作するため、Outlookユーザはすぐにでも CertCONNECTの利用が可能です。それ以外のメーラーについても今後適用を拡大していきたいと思います。特にスマホでの利用に関してはハードルが高いのですが、重要なメールには基本S/MIMEを付けておかなければならず、設定の有無がバラバラなのは意味がないので、スマホも今後対応できるようにしていきたいと思います。まずはPCでの適用が重要だと思います。

（4）ファイル送信方法

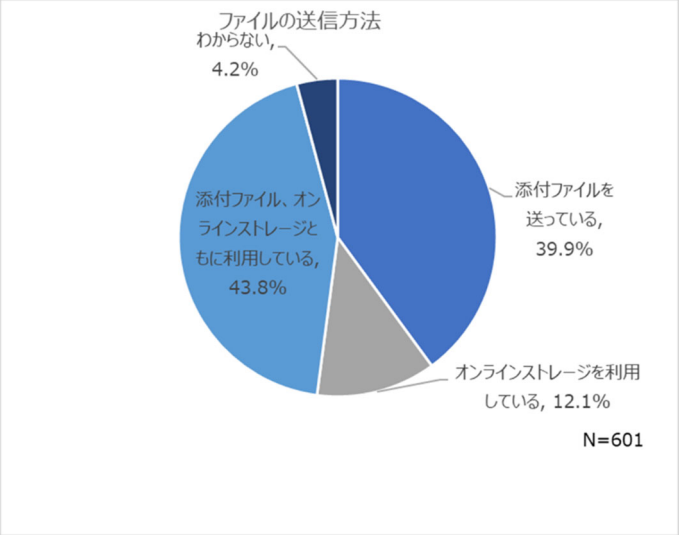


図14. ファイル送信方法

【稲葉】ファイルの送信方法として、添付ファイルを送る方法を利用されている割合が大きいですが、容量などによっては添付ファイルを受信側がはじいてしまうことがあります。添付ファイルとオンラインストレージの併用というのは、おそらく内容の重要性や添付ファイルのサイズによって、使い分けをされているのだと思います。
一つのアイデアとして、オンラインストレージへのアクセスはかなり便利だと思いますが、ストレージにアクセスするための情報、URLやパスワードなどを平文で送るよりもS/MIMEによる署名や暗号化を用いることにより、安全・安心の度合いが増すのではないでしょうか。

●PPAPの代替となる利便性のよいファイル送信方法について

【佐々木】PPAPに代わるメールでのファイル送信方法として2つ考えられます。一つは、クラウドストレージ対応です。先ほど稲葉さんがおっしゃたように、注意しながら利用する方法があります。
2つ目としては、環境がよくなれば、2者間でのS/MIMEの利用が考えられます。S/MIMEはまだ使いにくさがありますが、普及していくことで徐々に解決できるのではないでしょうか。
【大泰司】それぞれメリット／デメリットがある、ということですね。

●なりすまし対策事例について

【大泰司】先ほど、渡辺さんに事例をご紹介いただきましたが、補足をお願いします。

【渡辺】CertCONNECTにお問合せがありました中で、なりすましメールが来なくなるような対策を望まれている企業様から「S/MIMEを設定してCertCONNECTを導入すればなりすましメールは来なくなるのか？」とご質問がありました。残念ながらそれはできないので「なりすましメールか否かがはっきりわかりやすくなります」と回答しています。ウイルス対策などと同様に、なりすましメール受信をゼロにすることは難しいですが、御社のメールがS/MIMEを設定していることがわかるようになれば、なりすましはされにくくなるし、またS/MIME付きのメールがどんどん増えてくると、最終的になりすましそのものが減っていくのではないでしょうか。

【大泰司】最終的にはなりすましメールが来なくなることにつながると思いますが、まずは送信者として自分がなりすまされないことが重要です。

他に事例があればご紹介ください。

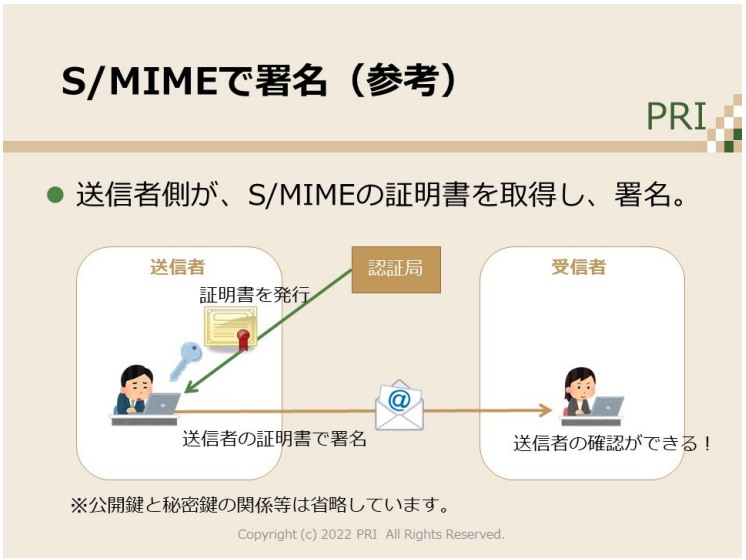
【JIPDEC佐藤】S/MIME導入事例として、JIPDEC、防衛装備庁、IPA、CSA Japanが全社的な導入を宣言されています。その他、全社的にではありませんが、一部の金融機関や省庁がメルマガ配信等にS/MIMEの電子署名を付けています。

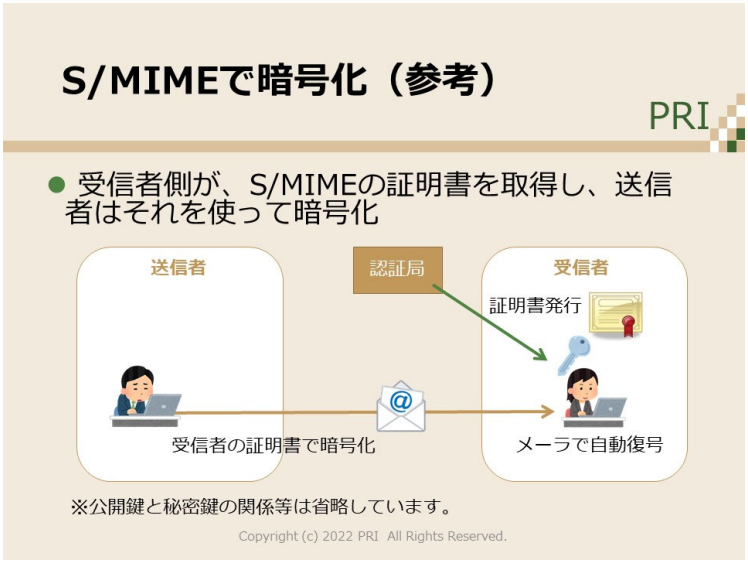
●S/MIMEが普及しない理由

【田上】S/MIMEについては、過去にJIPDECがいろいろと啓発をされていた経緯もあり、金融関係機関で、お客様用問合せ窓口だけS/MIME対応をされている、との事例紹介がありましたが、全社的に展開するにあたっては、証明書を発行する認証局というよりも、証明書の発行・インストール・管理・更新・失効ができる仕組みがないといけないのではないでしょうか。それが認証局の役目となるのか、サードパーティで展開するのか、CertCONNECTなどのソリューションを活用するのか。認証局は証明書を発行するのは得意でしょうが、デリバリーに関してはソリューション企業に依頼できないかと思います。

普及啓発については、JIPDEC、フィッシング対策協議会、認証局としても、セミナーなどで定期的に必要性を訴え続けることが重要なのではないでしょうか。今後も普及のリーダーとして必要性を訴えていきたいと思います。

● S/MIMEを利用した暗号化





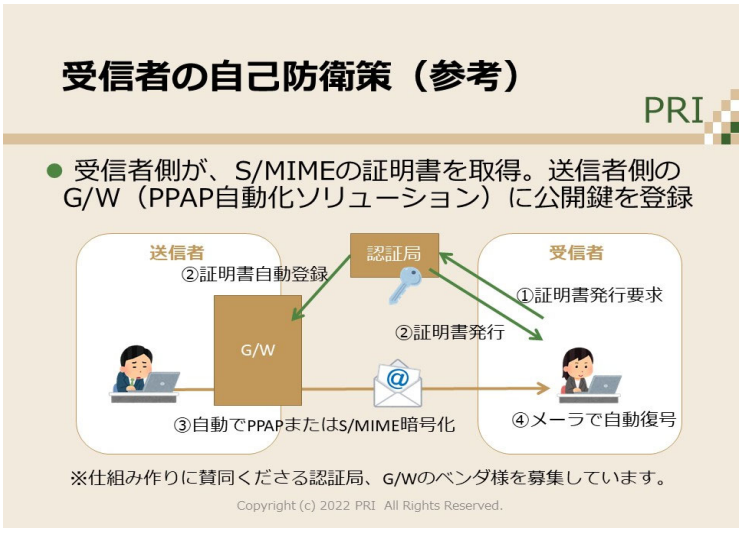


図15．PPAP用ゲートウェイを利用したS/MIME暗号化

【大泰司】署名は送信者がS/MIMEの証明書を取得しますが、暗号化の場合、受信者がS/MIMEの証明書を取得しなければならないため、ハードルが高いのです。
PPAPは、多くの場合、PPAP用ゲートウェイで自動的にPPAPを送信しています。受信者は、これを逆に利用して、自分の証明書をPPAP用ゲートウェイに登録させて、自動的にS/MIMEの暗号化をさせれば、自分に来るPPAPを減らせるのではないか？と思いますが、いかがでしょうか？
【稲葉】送信側が自分自身で証明書を持っていればできるのですが、やはり暗号化となれば受信者側の証明書がなければできないことになります。このようなゲートウェイがあれば非常に便利だと思いますが、ゲートウェイで受信者側の証明書をどうやって集めるのか、たとえば、弊社GMOグローバルサインの他、サイバートラスト社様、セコムトラストシステムズ社様などS/MIME用電子証明書をサービスラインナップに持つ認証局が発行しているS/MIME用電子証明書をどうやって集めるか、また使う時点で電子証明書が有効かの確認も必要でしょうし、運用面で何かあったときにどう対処するか等についても考えていかなければならないと思います。
署名は自身のアクションでできるのに対し、暗号化については、簡単には進められないと思います。一つの認証局だけではなく、さまざまな認証局同士、あるいはその証明書を扱うアプリケーションベンダーも含めて検討する余地があるのではないでしょうか。

●最後に
【田上】S/MIME、暗号化をどのように対応していくか、業界一丸となって取り組んでいくことが非常に重要であると思います。
【稲葉】S/MIME普及に向けてグローバルな動向把握に努めると共に、関連する業界とも連携して取り組んでいけたらと思います。
【渡辺】ユーザの立場、またソリューションを提供する立場として、S/MIMEを普及促進するためのツールとして、CertCONNECTをご紹介しました。大規模なユーザほど導入が難しいかと思いますが、ぜひこの仕組みを参考にしていただき、ビジネスマナーとしてS/MIMEを付けていただく状況になればいいと思います。
【高倉】地方企業など、これまで紙や電話、イントラネットの中だけで済ませられていた業務をインターネットでやりとりするようになることで、メールでの送受信が増えると思いますので、ぜひなりすましメール対策としてS/MIMEを導入していただきたいと思います。
【佐々木】本日の話を聞いて、S/MIMEの実用化・運用にはさまざまな障害があることに気づきました。義務化して100%普及してしまえば問題はないのですが、そこに行くまでの工程がなかなか難しい。暗号化については、クラウドストレージの利用、S/MIMEの双方向からアプローチしていくのが現状ではあるのだろうと思いました。引き続き勉強していきたいと思います。

以　上

PPAP総研
大泰司 章 氏

三菱電機、日本電子計算の営業現場で実際に数多くの企業や官公庁と商取引をする中で、紙にハンコ、PPAP（Passwordつきzip暗号化ファイルを送ります/Passwordを送ります/An号/Protocol)、PHS（Printしてから/Hanko押して/Scanして送ってくださいプロトコル)、ネ申エクセルといった形式的な電子化に苦しめられる。
これらの不合理な商習慣を変えるべく、2012年より一般財団法人日本経済社会推進協会（JIPDEC）にて電子契約やインターネットトラストを普及させる。
2020年からはPPAP総研を設立してユーザ向けとベンダー向けコンサルティング活動に従事。

フィッシング対策協議会 証明書普及促進WG　主査
（サイバートラスト株式会社　マーケティング本部
プロダクトマーケティング部）　　田上　利博 氏

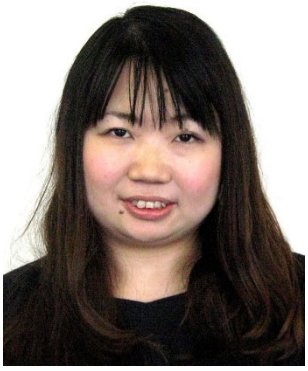
20年以上にわたりセキュリティベンダーで営業、プロダクトマーケティングに携わる。現在はサイバートラストで、認証・セキュリティ事業のプロダクトマーケティング全般を担当。デジタル改革関連法をはじめ、DX推進に影響のある法制度などの最新情報についても多数執筆している。フィッシング詐欺やドローン、IoTなどのセキュリティ課題にも取り組む。

フィッシング対策協議会 証明書普及促進WG　副主査
（GMOグローバルサイン株式会社　事業企画部）　稲葉　厚志 氏

・1990年代後半の電子認証事業黎明期よりPKI/電子認証に関わる事業開発に従事
・CA/Browser Forum、Asia PKI Consortium、ETSI Technical Committee Electronic Signatures and Infrastructures、デジタルトラスト協議会、トラストサービス推進フォーラム、JIIMA(公益社団法人日本文書情報マネジメント協会)等々の国内外協議会、フォーラムメンバーとしてガイドライン策定や啓発・提言活動に参画

九電ビジネスソリューションズ株式会社
ビジネスソリューション事業部ビジネスソリューション第2部 部長
渡辺　雅久　氏

九州電力に入社後、システム部門に30年以上従事し、多くの大規模開発プロジェクトやシステム導入・運用全般に関わる。2018年にOffice365導入プロジェクトに従事し、その中でS/MIME運用自動化の仕組みを九電グループ14,000名に導入。
2020年7月より現職。上記自動化の仕組みを2021年4月「CertCONNECT(サートコネクト)」としてサービス開始し、S/MIMEの普及拡大に励んでいる。ユーザ企業システム部門での長年の経験を活かし、お客さま目線で価値あるITソリューション提案に励んでいる。



一般財団法人日本情報経済社会推進協会（JIPDEC）
セキュリティマネジメント推進室　主査　高倉　万記子

JIPDECデジタルトラスト評価センター兼セキュリティマネジメント推進室主査。トラストサービスやインターネット上のなりすまし対策の普及啓発を行っている。

本内容は、2022年2月18日に開催されたJIPDECセミナー「S/MIME最前線「なりすましメール対策の現状と課題－S/MIMEを活用したなりすまし対策事例紹介」」パネルディスカッションの内容を取りまとめたものです。