BIMIの対応って大変なの？
～BIMI対応企業パネルディスカッション

モデレーター　：日本スマートフォンセキュリティ協会/KDDI株式会社　本間 輝彰
パネリスト　　：デジサート・ジャパン合同会社　林 正人
楽天グループ株式会社　高田 加菜江
株式会社TwoFive　伊藤 隼人
KDDI株式会社　蔡 京泰

JSSECとは？

JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人 日本スマートフォンセキュリティ協会　略称：JSSEC=じぇいせっく

会長　佐々木 良一　（東京電機大学 名誉教授 兼 サイバーセキュリティ研究所 客員教授）

スマートフォンの**安全な利活用を図り普及を促進**するために、2011年5月に任意団体としてスタート
2012年4月より一般社団法人として活動
その他、**IoTやICTの安心安全な**普及啓発活動

JSSEC が目指すもの

スマートフォンは社会のさまざまな場所において利活用が進んでおり、今や社会と人をつなぐ有用な役割を果たしています。
IoT（モノのインターネット）の拡大により、従来では考えられなかったあらゆる「モノ」がインターネットに繋がる世界となり、さらに社会を変革しようとしています。その**社会と人の接点になるのが、スマートフォンなどのスマートデバイス**です。
JSSECは、この人との接点となるスマートフォンなどを中心に、この新たな社会での更なるセキュリティの重要性について普及啓発してまいります。

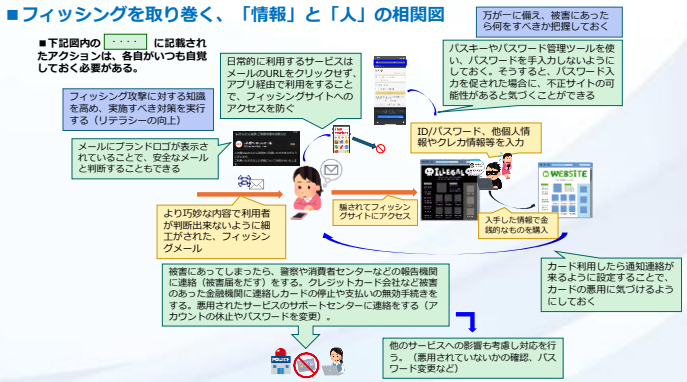
「スマホ利用シーンに潜む脅威 Top10」

スマートフォン利用シーンに潜む脅威 TOP 10/2023	
第１位	依然猛威を振るうスミッシング詐欺
第２位	なりすまし契約とアカウント詐取
第３位	ディープフェイク
第４位	メールを狙った様々な攻撃 ～フィッシングメール・ビジネスメール詐欺、 ランサムウエアの脅威など～
第５位	提供元不明アプリによるマルウェア感染
第５位	誹謗・中傷
第７位	SNSフェイクニュース
第８位	アカウント乗っ取りと誤ったアカウント登録
第９位	検索エンジンの汚染
第10位	不正通販サイト
ランク外	不適切なパスワード管理
	アプリストアのマルウェア感染
	スマホカメラの悪用
	短縮URL問題
	盗難・紛失

https://www.jssec.org/report/news20230228.html

フィッシング ・スミッシング メール対策ガイドを公開

https://www.jssec.org/smartphone-use-10threats202301



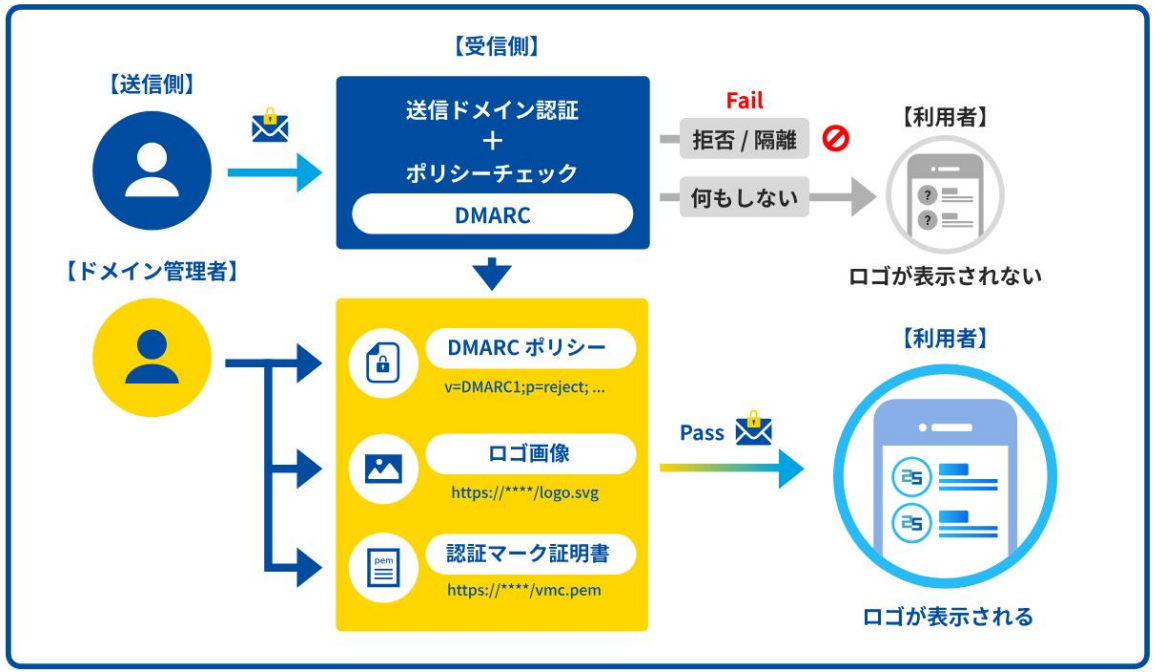
Agenda

- BIMIの概要とBIMI導入のメリット（プレゼン） 自己紹介を含めて10分
- BIMI対応の苦労話（パネル） 15分
- 実際にBIMI対応してみて（パネル） 15分
- 質疑応答 5分

BIMI概要とBIMI導入のメリット

BIMIとは

BIMI（Brand Indicators for Message Identification）とは、メールの認証技術の一つで、企業やブランドが送信するメールに対して、そのブランドのロゴを表示することを目的としています。これにより、受信者は視覚的にメールの信頼性を確認出来るようになり、フィッシングのリスクを低減することが可能となる



https://www.twofive25.com/service/bimi.html

【前提条件】

- DMARCを導入し、**BIMIの仕様に満足した条件**で**p=quarantine または p=reject**（p=rejectが推奨）のポリシーでDMARCレコードをDNSサーバに登録し公開する
- 表示するロゴは商標登録を行い、VMC （Verified Mark Certificates）証明書を取得する
- 取得したVMC証明書とロゴファイル（SVGファイル）をWeb公開する
- BIMIレコードをDNSサーバに登録し公開する

【認証流れ】

- DMARC認証を行い、BIMIの仕様にマッチした条件でDMARC認証を“Pass”する
- BIMIレコードの有無を確認する
- VMC証明書とロゴファイルを取得し、証明書の検証を行う
- 検証が“Pass”したらロゴ表示する（**ロゴ表示の有無は、メールクライアントの対応有無に依存**）

VMC証明書の安全性

JAPAN SMARTPHONE SECURITY ASSOCIATION

VMC証明書は、CA（認証機関）として信頼度の高い**DigiCert社**と**Entrust社**の２社のみの発行となっており、且つ、下記に示す通り厳格な審査のもと発行されるため、**攻撃者やペーパーカンパニー等**がVMC証明書を取得するのは**不可能**と言える

VMC証明書発行条件（申請者に求められる条件）

- **法人としての存在**：登録機関に申請して法人として認められている必要がある（法人設立証明書や登録番号などが必要）
- **登録代理人とオフィスの指定**：登録機関に登録代理人やオフィスを指定している必要がある
- **活動状態**：「非活動」「無効」「現在ではない」などのラベルが付いていないことが必要
- **実体があること**：実際に存在し、ビジネス活動を行っている必要がある
- **事業可能地域**：組織の設立や営業を行っている場所が、法律で禁止されている国でないことが必要
- **禁止リストに掲載されていないこと**：政府の禁止リストや制裁リストに載っていないことが必要
- **ロゴの商標登録**：表示するロゴを商標登録を行う

VMC証明書審査条件（CAが申請者に対する審査条件）

- **申請者の確認**：申請者が法的に存在し、正しい身分であるか、実際に物理的な場所でビジネスを行っているか、実際にビジネス活動を行っていることを確認する
- **ドメイン名の確認**：証明書に含まれるドメイン名を申請者が所有しているか、管理していることを確認申請者が法的に存在し、正しい身分であることを確認する
- **連絡手段の確認状態**：証明書に記載される組織との信頼できる連絡手段があるかを確認する
- **証明書の承認確認：**証明書の申請が正当に承認されているか、契約にサインした人の名前、役職、権限を確認し、利用規約に同意したことを確認し、申請を承認したことを確認する
- **ロゴの承認**：
  - **商標登録の確認**：申請者が提供した商標登録番号や登録機関の名前が、公式データベースで有効であることを確認する
  - **商標の所有権確認**：商標の所有者が申請者と同じであること、または申請者がその商標を利用する権利を取得していることを確認する(**所有者が異なる場合は、所有者からの承認が必要となる**)
  - **マークの一致確認**：申請されたマークが登録商標と一致しているかを確認する
  - **色の制限**：商標の色は、登録商標で許可されている色のみ使用されているか確認する

Minimum Security Requirements for Issuance of Mark Certificates　https://bimigroup.org/resources/VMC_Requirements_latest.pdf

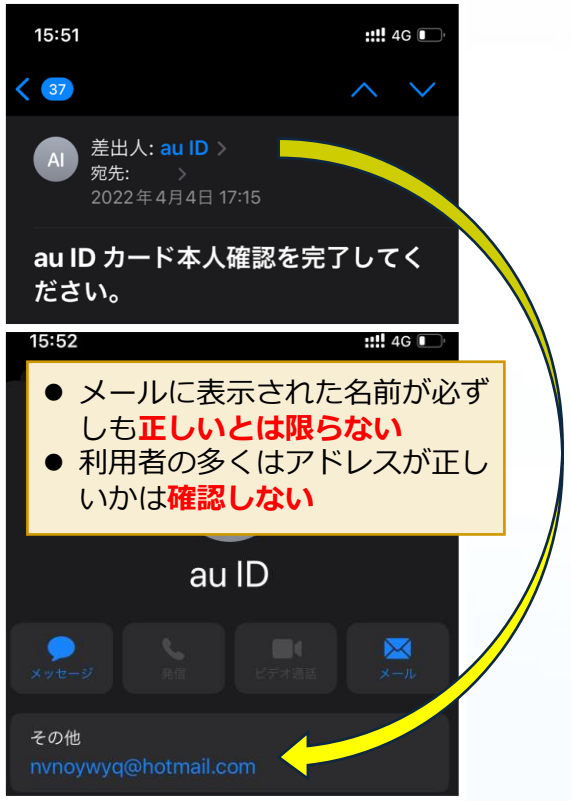
BIMIがなぜ必要となるか

DMARCは送信されーたメールが正規の送信元から送信されているか識別する技術（**送信元がなりすましされていないかを識別する技術**）

攻撃者もDMARCに対応して送信すれば、DMARC認証は“**Pass**”する

DMARCの認証結果のみで**フィッシングメール対策とするのは不可能**

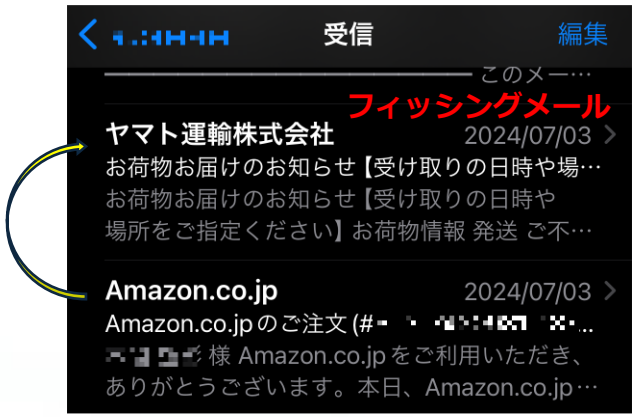
ディスプレイネーム問題



- メールに表示された名前が必ずしも**正しいとは限らない**
- 利用者の多くはアドレスが正しいかは**確認しない**

フィッシングメールに使うドメインは何でもよい

フィッシングに騙されやすい事例



タイミングよく関連のメールを受信するとそのメールを正規なメールと判断してしまう

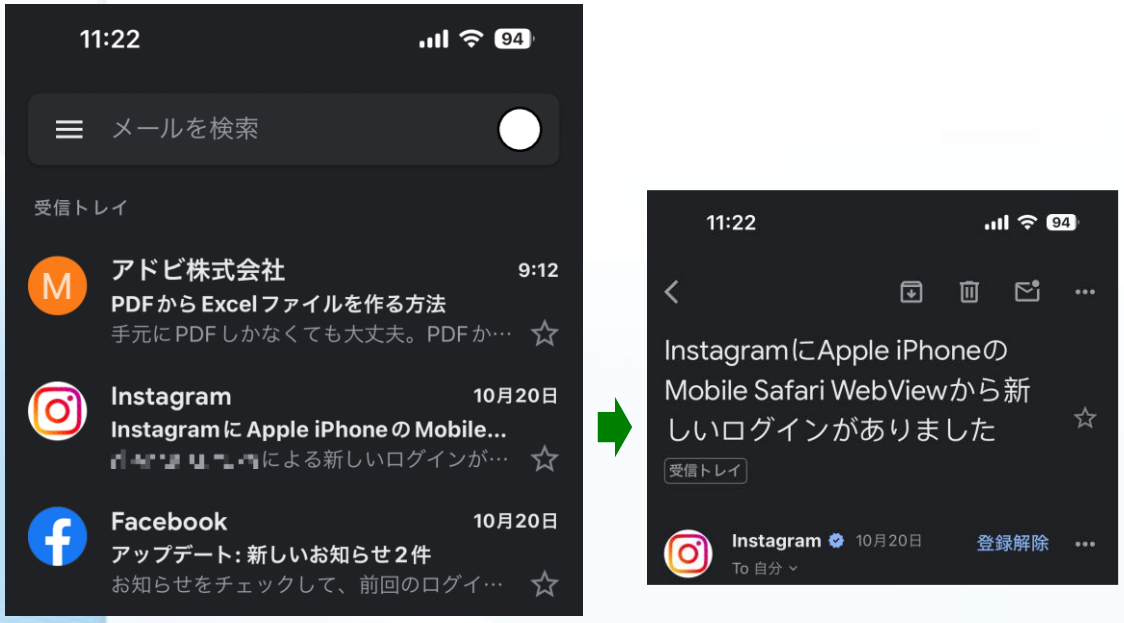
従来の技術で利用者にフィッシングメールで気づかせることは困難

- 全ての利用者にメールを注意深く確認させることは不可能

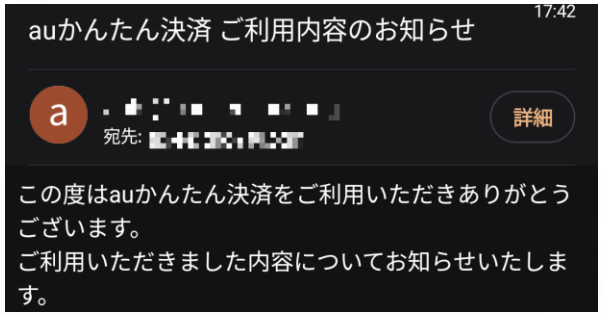
BIMIに対応すると

利用者は、ロゴ表示されているメールは安全なメールと認識するだけで、安全なメールの識別が可能となる

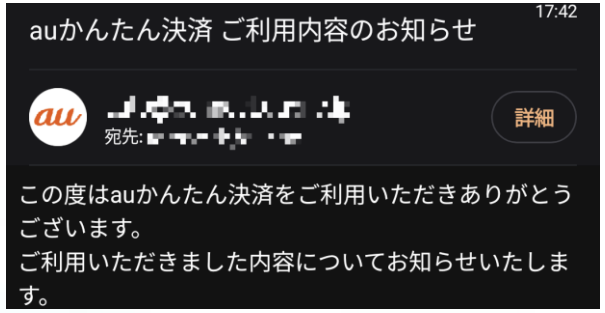
【Gmail BIMI対応】



【iPhone BIMI対応前】



【iPhone BIMI対応後】



よく言われる推奨されるフィッシング対策

- フィッシングメールかどうかを判別はしない
- URLリンクをクリックせずアプリからの利用やブックマークからアクセスをする

対策としては正しいが、**利用者視点では面倒**

したがって、安全なメールだけを識別させてあげれば、**利用者の負荷は軽減**するのでは？

メールを送信する目的 – メールを読んでもらうこと

利用者にメールを送る目的は、利用者に対して重要な情報や有益な情報を案内し、利用者への確認や自社サービスに誘導することである

いいかえれば、利用者に**メールを読んでもらう**ことが最大の目的である

利用者に自サービスからのメールであり、且つ、安心なメールであるとうことが識別出来れば、利用者の興味がある内容であればメールを開封してもらえる確率が上がると推測される

多くのメールを受信すると、読んで欲しいメールが埋もれてしまい、気づかない可能性が出てくるが、ロゴ表示することで気づかせることが可能となる

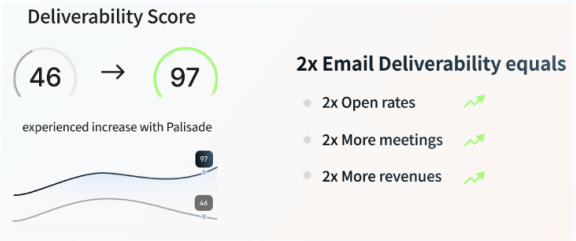
BIMIによるブランディング効果事例

BIMI対応しメールにブランドロゴを表示することで、企業はブランド認知度を高め、メールの配信能力を高め、利用者の信頼性を高めることが可能と言われており、**2024年７月**にPALISADEより、**メールの配信率、メールの開封率、ブランド想起率が向上**されたという結果が報告されている

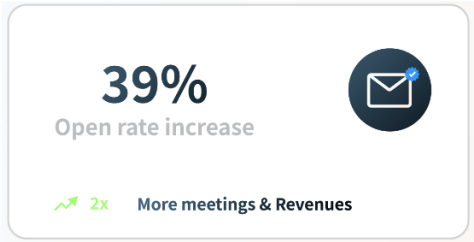
How to improve your open rates by 39% with BIMI

July 2, 2024

メール配信能力



メールの開封率



ブランド想起率

https://www.palisade.email/resources-post/how-to-improve-your-open-rates-by-39-with-bimi

gaiiaでは、カンファレンスのデモ予約率が21%向上という結果も出ている

Case Study: We increased gaiia's open rate by 43%.

gaiia CASE STUDY

July 2, 2024

開封率

35%→50%（43%向上）

予約率

カンファレスのデモ予約率が向上

https://www.palisade.email/resources-post/case-study-we-increased-gaiias-open-rate

2021年のEntrust社の調査結果でも、開封率が21%増加、平均購入の可能性が34%増加、ブランド想起が18%増加したというデータも公開されている

https://www.entrust.com/blog/2021/08/consumer-interaction-improves-when-emails-display-logo-testing-reveals/

BIMI対応サービスのカテゴリー例

JAPAN SMARTPHONE SECURITY ASSOCIATION

グローバル見た場合は、BIMI対応企業のカテゴリは、フィッシング詐欺に狙われやすいカテゴリ以外のカテゴリも多く対応している

金融関連	マーケティング／データ分析	アパレル	ソフトウェア関連	ヘルスケア関連	医療関連	IT ソリューション	**保険関連**	セキュリティ	エンターテイメント
86	35	33	32	32	25	25	24	21	19

教育	観光業	メディア	不動産	**EC**	フード関連	**銀行**	テクノロジー	**通信**	エネルギー関連
18	18	18	16	15	14	14	14	13	11

クレジット	**物流**	投資関連	**ソーシャルメディア**	コンサルティング	製造	ジュエリー	クラウドサービス	求人	**デジタル決済**
10	10	10	9	9	9	7	6	6	6

家電	家具	テレコミュニケーション	教育関連	建築関連	専門団体	交通	バイオテクノロジ	ゲーム関連	書籍関連
6	6	6	6	6	5	5	5	5	5

赤太字は国内でフィッシング詐欺に狙われやすいカテゴリー

参考データ：なりすまし対策ポータル ナリタイ　BIMI対応組織リスト　https://www.naritai.jp/enterprise_bimilist.html

国内のBIMI対応サービス

auPayカード	クレジット
イオンカード	クレジット
エムアイカード	クレジット
Orico	クレジット
JCB	クレジット
東急カード	クレジット
VIEWカード	クレジット
PayPayカード	クレジット
三井住友カード	クレジット
三井住友カード	クレジット
ライフカード	クレジット
楽天カード	クレジット
LuVit	クレジット
UCSカード	クレジット
auじぶん銀行株式会社	銀行
ソニー銀行	銀行
PayPay銀行	銀行
三井住友銀行	銀行
楽天銀行	銀行
ゆうちょ銀行	銀行
横浜銀行	銀行
auPay	電子決済
WebMoney	電子決済
Paidy, Inc.	電子決済
楽天ペイ	電子決済

かんぽ生命保険	生命保険
au損保	損害保険
楽天保険	損害保険
アコム	金融ローン
外為どっとコム	FX
au	通信
KDDI	通信
Povo	通信
J:Com	CATV
楽天	EC
Yahoo!	EC
カイゴジョブ	求人
ジョブメドレー	求人
楽天トラベル	旅行予約
一休.com	ホテル予約
アソビュー	観光
U-NEXT	エンターテイメント
ベビーカレンダー	育児
暴露王	ギャンブル
WORLD	ギャンブル
Diptyque	香水
カクヨミ	電子書籍
DLsite	電子書籍
めちゃコミック	電子書籍
Skeb	イラスト

パワーソリューションズ	DXコンサル
アジアクエスト	DXコンサル
WOW WORLD	メールマーケティング
READY FOR	クラウドファンディング
HENNGE	クラウドセキュリティ
Trend Micro	セキュリティ
Brand Keeper	ホスティングサービス
さくらインターネット	ホスティングサービス
freee K.K.	法人ソフトウェア
SmartHR	法人ソフトウェア
TwoFive	SI
椿本チエイン	製造
彌満和製作所	機械工業
CANDY HOUSE JAPAN	スマートロック
国際ビジネスコミュニケーション協会	英語教育
プレミアムバンダイ	ホビー

フィッシングメールに狙われやすいサービスを中心に、それ以外のサービスにもBIMIが普及しつつある

参考データ：なりすまし対策ポータル ナリタイ　BIMI対応組織リスト　https://www.naritai.jp/enterprise_bimilist.html

BIMI対応の苦労話

BIMI対応の苦労話

JAPAN SMARTPHONE SECURITY ASSOCIATION

- BIMI対応する際の、DMARC対応の苦労

DMARC親ドメインの対応が必須
サブドメインがDMARC Failになる問題
ポリシーをQuarantine/Rejectへどう行ったか

- VMC証明書の取得での苦労

ロゴの問題（商標登録、画面イメージ）
証明書の更新問題

- 送信ドメイン認証の問題

DKIM対応必須
DKIM第三者認証NG（配信事業者利用時の注意）
SPF記述ミス（include管理）
DKIM tタグ

SPF/DKIM設定

BIMI導入に際して必要とうなるDMARC（DKIM/SPF)においても設定上の問題が散見される

□ SPF include問題

- SPFレコードで参照している、include先の**SPFレコードが参照不可**の場合がある。メールサーバの仕様にもよるが、SPFの認証結果がPermErrorとなり、BIMI/DMARCの認証結果に影響を与える可能性がある。したがって、includeを使っている場合は、そのドメインが存在しているかを**定期的に監視**することが重要
  - 65,000ドメイン調査した結果、453ドメイン（**0.7%**）に記載不備が見つかった
- その他にも**SPFの記述が間違っている**ドメインがいまだ散見されるのが実態

□ DKIM tタグ設定

- DKIMのパラメータに署名実施時のタイムスタンプを設定する“tタグ”を送信することが可能だが、**送信側のサーバと受信側のサーバの時刻があっておらず“PermError”**となるケースがある
  - NTPサーバによる時刻同期を意識されることはあまりなく、送信側のサーバで大きく時刻がずれているケースがある（NTP同期をしない場合、**１日に約10分から1時間程度のずれが発生する**と言われている）
  - DKIMのRFC6376の3.5. The DKIM-Signature Header Fieldに、 INFORMATIVE NOTEとして時刻が一致しない場合があるので、 “fudge factor”を設定してずれを許容してもよいとなっているが、あくまでもMayの記述であり、受信側が“fudge factor”を設定していても、どのような時間を設定しているかは受信側次第であるため、送信側での**時刻同期が出来ているか確認**する必要がある

RFC 6376 - DomainKeys Identified Mail (DKIM) Signatures より
INFORMATIVE NOTE: Due to clock drift, the receiver's notion of when to consider the signature expired may not exactly match what the sender is expecting. Receivers MAY add a 'fudge factor' to allow for such possible drift.

実際にBIMI対応してみて

実際にBIMI対応してみて

JAPAN SMARTPHONE SECURITY ASSOCIATION

- どのような効果があったか
  - 開封率の話し
  - DMARCが普及した（ロゴ表示要望）
  - その他
- VMC証明書の保存先
  - Webサーバの設定
  - ※自作自演DDoS攻撃
  - ※キャッシュ時間の問題
- 要望
  - BIMI対応していないサービスへの要望

VMC証明書・SVGファイルの管理

VMC証明書・ロゴファイルの公開元のサーバは、VMC証明書の発行元であるDigiCert社、Entrust社のサーバで公開するケースと自社HPなどに公開するケースの２つに分かれる。この内、**問題が出るのは自社HPなどに公開**している場合となる

DigiCert	Entrust	その他
27.7%	35.5%	36.8%

※：KDDI調査結果より（調査数853）

□ no-cache/no-store/max-age=0 の設定

- これら設定はキャッシュをさせない、有効性を都度確認させることを目的に利用される設定だが、メルマガ等短時間に大量にメールを送信する場合、**mail by mailでWebサーバへの問合せが発生**しHTTP- DDoSの攻撃を受けている状態に陥るケースがある。場合によっては、Webサーバでアクセスがブロックされ、BIMI認証失敗となるケースも考えられる（受信側からすれば、都度DNSに問合せするのは不要な不可であり、これら設定を行うべきではない）。

□ 大きな値のmax-ageの設定

- max-ageで設定したキャッシュ時間の設定が非常に大きい（1年以上、長いものでは10年）のものが存在している。 この設定自体は問題ないが、**キャッシュ保持時間中にVMC証明書の有効期限を過ぎる**と、証明書の検証が失敗することなる。そのため、キャッシュ保持時間は適切に管理する必要がある。

VMC証明書・ロゴファイルの公開元のサーバをどこにするかは各社のポリシーに委ねられるが、適切に運用するためには、適切な設定がされていると推測される、**VMC証明書発行元のサーバで公開**することも検討することが推奨される。自社サーバで公開する場合は、**メールサーバ側の負荷なども考慮し、適切なパラメータを設定**することが求められる。また、VMC証明書専用のWebサーバに証明書を保存し、個別の設定を実施するなどの対応も検討すべきであると考える