JPAAWG 8th General Meeting

BIMI導入の最前線　ー　成果・課題と最新動向

日本スマートフォンセキュリティ協会　副会長・理事
KDDI株式会社　アプリケーション開発部　エキスパート
本間 輝彰

JSSECとは？

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。

自己紹介

本間 輝彰

一般社団法人 日本スマートフォンセキュリティ協会（JSSEC) 副会長・理事
KDDI株式会社　パーソナルシステム本部　アプリケーション開発部

KDDIにおいて、auおよび各種団体を通じて国内の迷惑メール対策を推進。その後、スマートフォンやIoTのセキュリティ対策、サイバー犯罪対策の推進に従事。

2016年よりJSSECに幹事として参加し、2020年からは副会長・理事に就任。技術部会や利用部会を通じて、スマートフォンの安全な利用を推進しています。最近では、フィッシング詐欺やディープフェイクなど、利用者を巧みに狙う詐欺に注力して活動しており、コラム執筆を通じてこれらの課題についても発信しています。
また、なりすまし対策ポータルサイトにおいて、BIMI対応組織リスト作成情報の提供も実施中。

- セキュリティコラム（2025年4月～）
  - 25年9月号：「課題が残る送信ドメイン認証の導入・運用」
    https://www.jssec.org/column/20250930.html
  - 25年7月号：「メールなりすまし対策強化 ― BIMIの現状について」
    https://www.jssec.org/column/20250731.html

なりすまし対策ポータル ナリタイ　MENU
なりすましを知れば、セキュリティの現在がわかる！
https://www.naritai.jp/

- 「BIMIについて」
  - https://www.naritai.jp/effectiveness_of_bimi.html
- BIMI 対応組織リスト
  - https://www.naritai.jp/enterprise_bimilist.html

なぜBIMIが必要か ― 人の脆弱性の課題

人間は多種多様なバイアスによって行動することが多い。バイアス自体が悪ではないが、詐欺を行う人は、**負の面のバイアス**をうまく利用し騙すことを行うことが多々見受けられる。

根拠なく信頼（信用）出来る人・機関からの情報と思い、疑いもなく信じてしまう

信頼のバイアス

根拠なく楽観的に物事を判断してしまい、過信から油断してしまう

過信のバイアス（ポジティブバイアス）

無知または無警戒
目先の利益への欲求
情報の提供に対する無批判な姿勢
ソーシャルエンジニアリングへの脆弱性

欲望のバイアス

限定品、いまだけなどお得感を与える、早急なアクションして行動してしまう

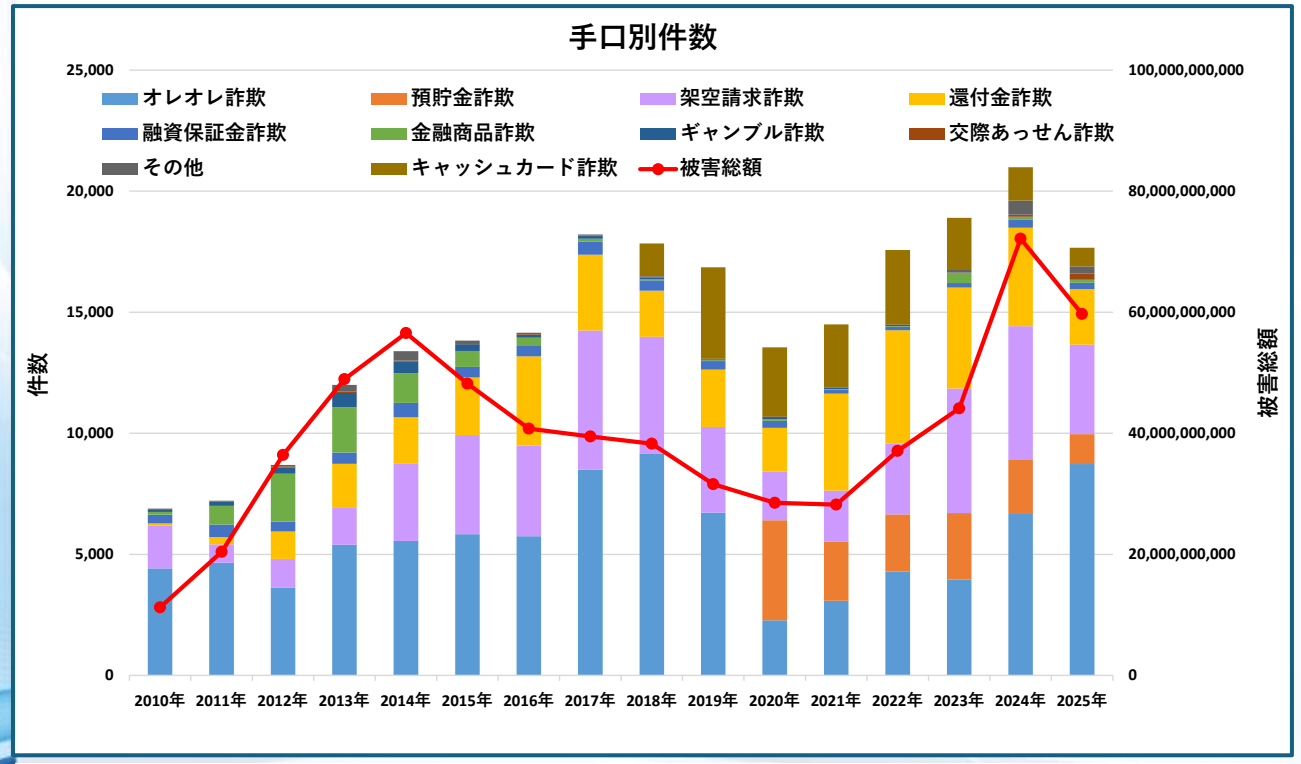
損失回避のバイアス(ネガティブバイアス)

根拠なく不安毎に対して、必要以上に過敏に反応してしまい、冷静な判断が出来なくなる

“虚構”を信じるという（騙されて（信じて）行動する）行為は、人間が持っている**本能の1つ**であり、これを防ぐことは不可能に近い？

なぜBIMIが必要か ー 人の脆弱性の課題

オレオレ詐欺など特殊詐欺の**被害件数**はコロナ以降再度**上昇**しており、被害額も右肩上がりで増加している。さらに**被害は年代・性別を問わず**発生しており、**ネットが普及した現在でも（逆に現在だから）人は容易に騙されてしまう**ことを実証していると思われる。



特殊詐欺及びSNS型投資・ロマンス詐欺の　認知・検挙状況等について（**2025年8月現在**）ー　警察庁
https://www.npa.go.jp/publications/statistics/sousa/sagi.html

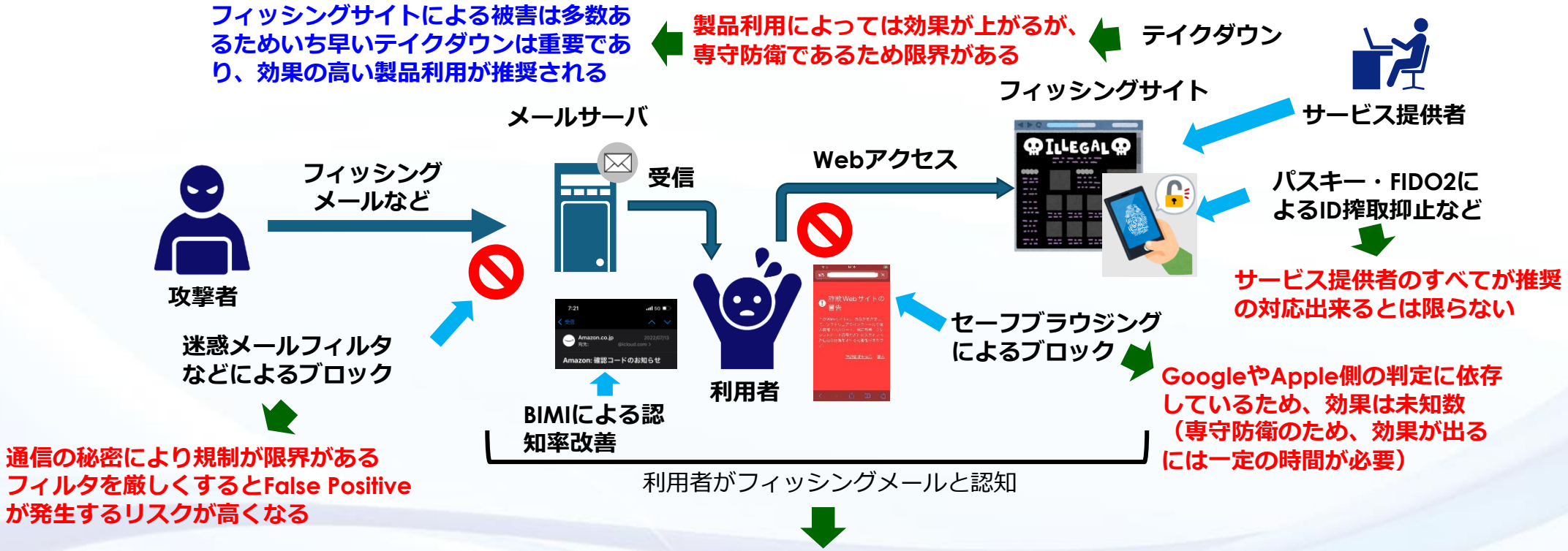
	男（%）	女（%）	合計（%）
１９歳以下	0.3%	0.2%	0.5%
２０～２９歳	5.8%	5.3%	11.1%
３０～３９歳	6.1%	4.80%	10.9%
４０～４９歳	4.3%	4.0%	8.3%
５０～５９歳	4.8%	4.8%	9.6%
６０～６４歳	3.4%	3.2%	6.6%
６５～６９歳	4.6%	5.1%	9.7%
７０～７９歳	7.8%	11.0%	18.8%
８０～８９歳	5.6%	16.6%	22.2%
９０～９９歳	0.8%	1.4%	2.2%
１００歳以上	0.0%	0.0%	0.0%
合計	43.50%	56.50%	

特殊詐欺の被害はご年配の方が多いと思われる方が多いが、実際には若年層の被害も比較的多いのが実態

なぜBIMIが必要か ー フィッシング対策の課題

複数の技術による対策を盛り込むことで、フィッシングメールによる被害の削減を行っているが、100%防ぐことは非常に困難な道のりである

➡ セキュリティ対策は、リスクの回避、軽減、移転、受容を有効的に行う必要がある。



対策の最後は、脆弱性のある利用者による認知に頼らざる得ないのが現実

なぜBIMIが必要か ー利用者へ提供すべき対策は

セキュリティ対策を進める際には、利用者が**日常の中で負担なく使える仕組み**が求められる。面倒な作業や手間が増える対策は、利用者の理解や協力を得にくく、結果的に効果が薄れる可能性がある。そのため、なるべく**自然な形で安全性を確保できる方法**を目指すべきである。

【BIMIの優位性】
利用者は**セキュリティの知識は必要なく、ロゴ表示されたメールのみ安全であると認識**すればよい

GMO BRABD SECURITYの調査ではロゴ表示されることで利用者の**75%が正当なメール**と感じている。
BIMIの訴求が進むことで、さらなる理解向上が期待できる。

GMO BRABD SECURITY
企業ロゴ付きメール（BIMI)に関する長さ結果報告（対象者：メール受信者）
https://brandsecurity.gmo/news/post/post-20250902/

“**メールアドレスを確認する**”、“**メールのリンクは使わず検索結果からアクセスする**”などは、フィッシング対策として効果はあるが、すべての利用者が対応する可能性は低いと言わざる得ない。**自分がやらない・やりたくない対策は推奨すべきでない**（誰もが理解できるセキュリティ対策の提供が必要）

BIMIの安全性　ー　真正性・信頼性・完全性の確保

BIMIは、情報セキュリティ７大要素の内、真正性・信頼性・完全性が保証された技術となっており、ブランドロゴが表示されたメールは極めて安全性が高いメールとなっている

セキュリティ要素	対策	内容
完全性：availability	DKIM	メール内容の改ざん防止
真正性：authenticity	DMARC	ヘッダFromドメインの正当性の証明
信頼性：reliability	VMC/CMC	ブランドの証明と保証

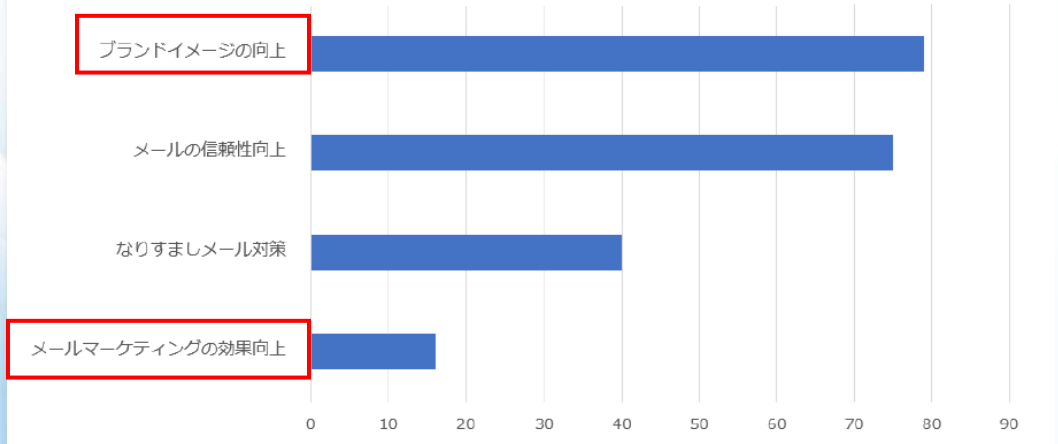
VMC/CMCの証明書発行事業者は、「**Minimum Security Requirements for Issuance of Mark Certificates** * 」に遵守した手順での証明書の発行が義務図けられており、**ペーパーカンパニーや攻撃者が取得するこは事実上不可**となっている
（サーバ証明書の１つであるEV証明書（Extended Validation）と同との審査に加え、表示するロゴは商標登録もしくは（CMCのPrior Use Mark Certificatesの場合）先使用を証明が必要となる

* https://bimigroup.org/resources/VMC_Requirements_latest.pdf

BIMI導入のさらなる目的

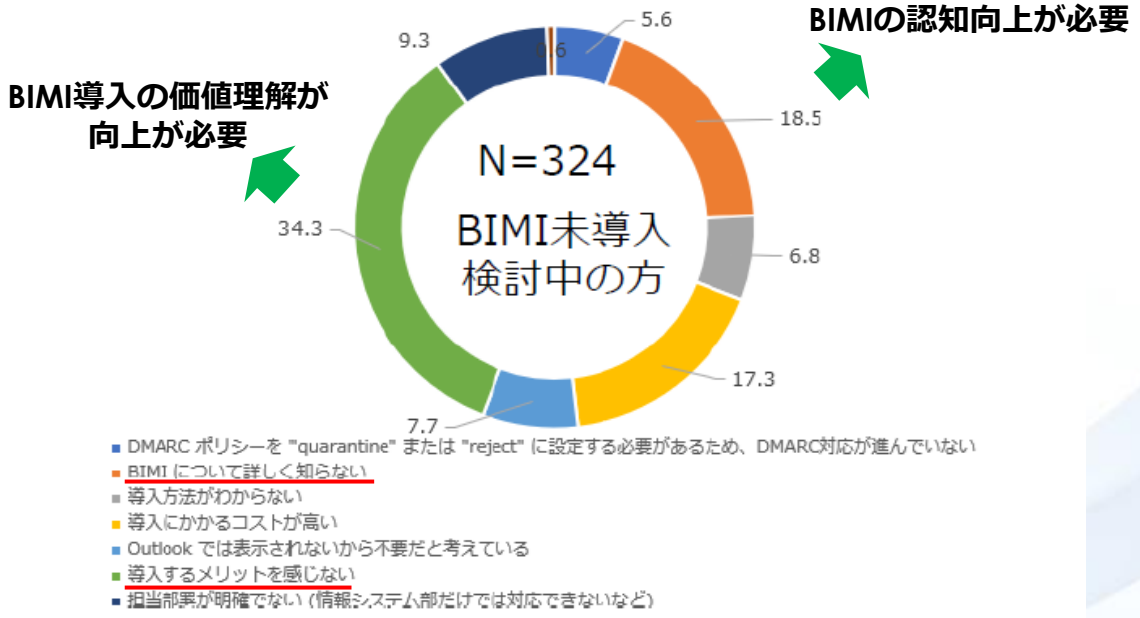
BIMI導入による効果は、フィッシング対策もあるが、それ以上にブランドイメージの向上が期待されている。

BIMI 導入によって、どのような効果を期待していますか？



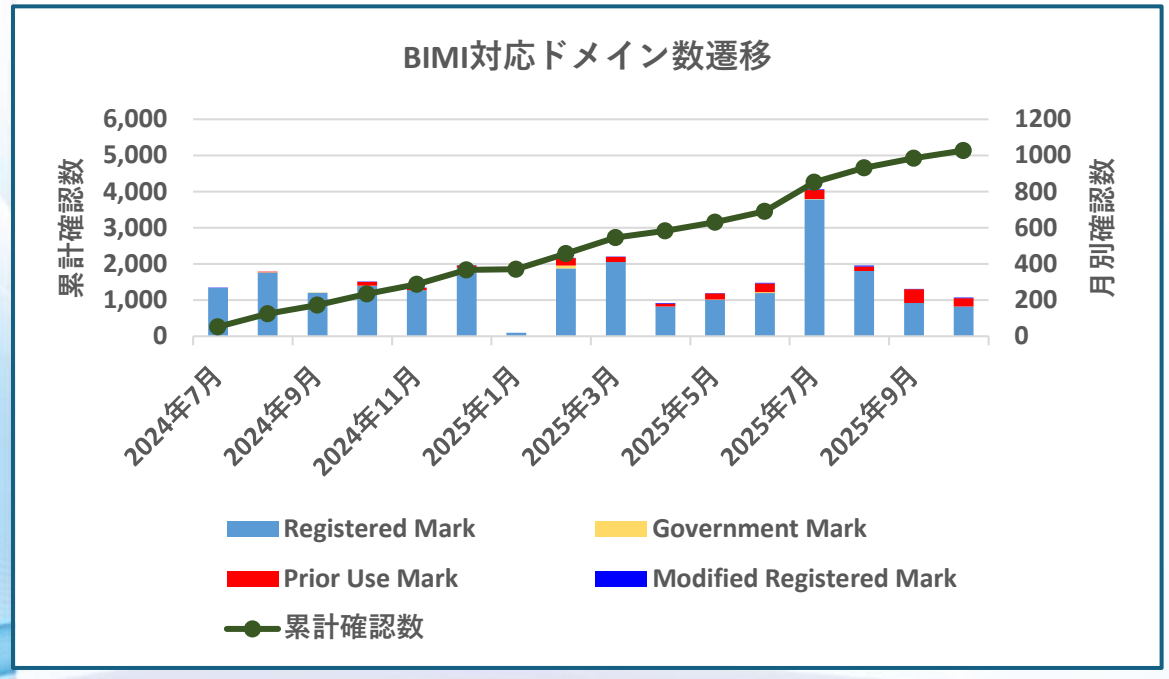
GMO BRABD SECURITY
企業ロゴ付きメール（BIMI)に関する長さ結果報告（対象者：メール配信者）
https://brandsecurity.gmo/news/post/post-20250902/

BIMIを導入していない（または検討中）の理由

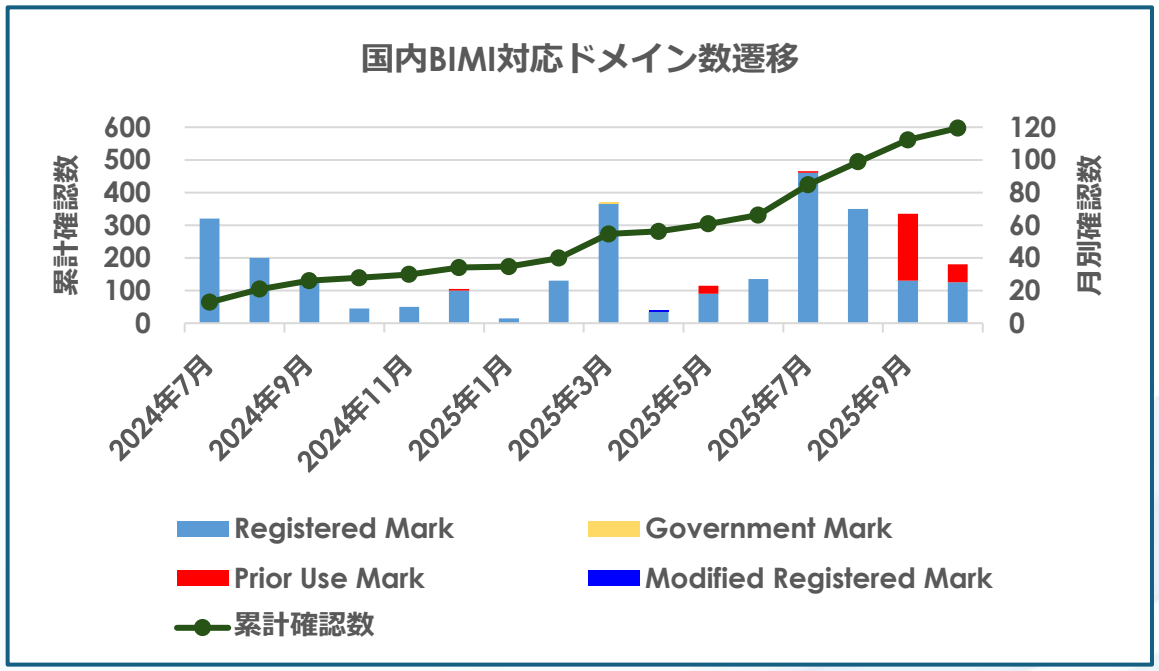


BIMIの普及状況について

BIMI導入によるフィッシング対策効果に加え、ブランドイメージ向上などメリットもあるため、BIMI対応ドメインは徐々に増えつつあり、なりすまし対策ポータルサイトナリタイでの調査結果では、約4,700超のドメインでBIMI対応を確認している。同様に国内ドメインも増えつつあり、450超のドメインがBIMI対応している。



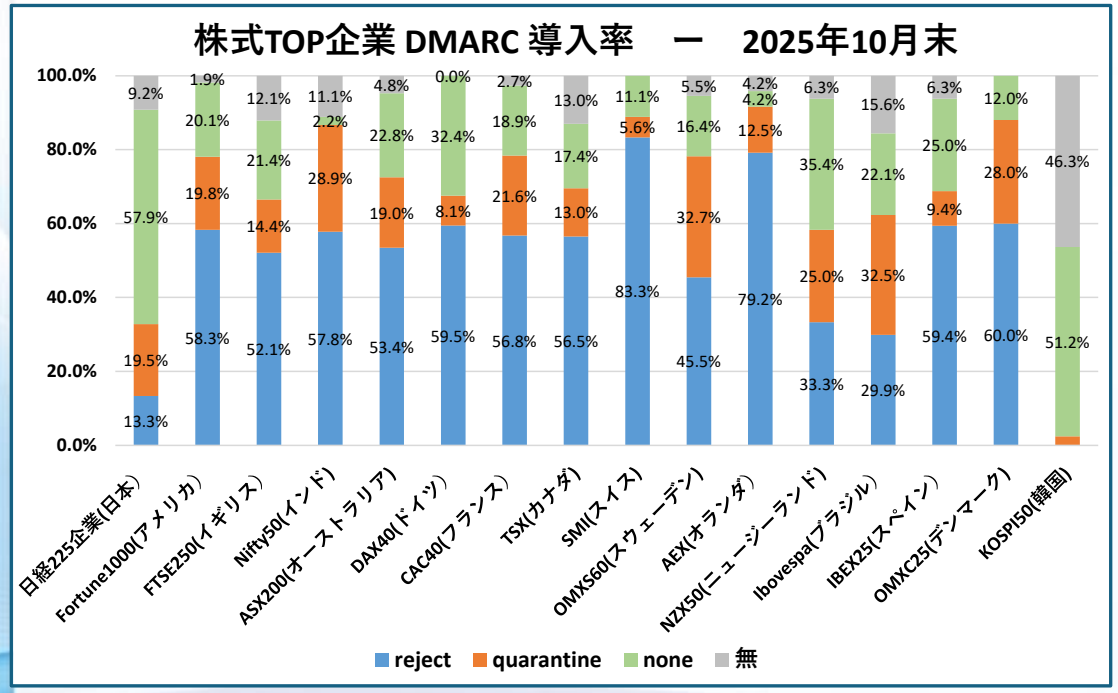
※ JSSEC調べ



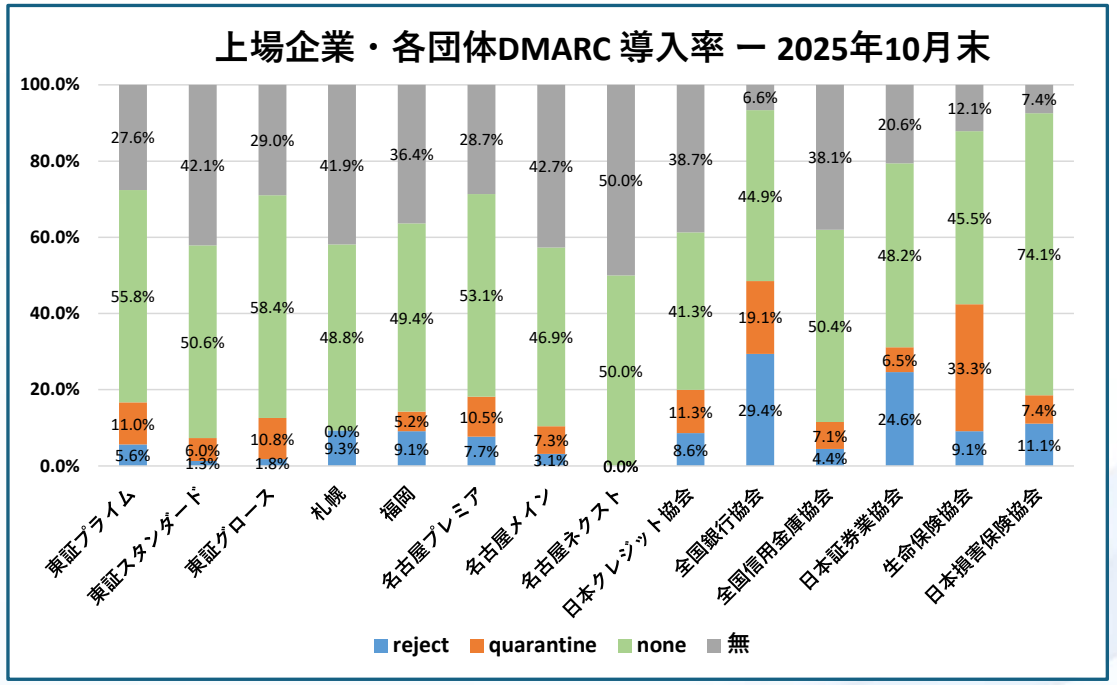
※ JSSEC調べ

BIMI普及に向けての課題 – 国内の低いDMARC普及率

各国の主要企業と比較すると、国内のDMARCポリシーはrejectやquarantineの対応がかなり劣っている結果となっている。国内の上場企業や金融関連団体においても、DAMRCポリシーのrejectやquarantineの対応は同様に低い結果となっている。



※ JSSEC調べ



※ JSSEC調べ

※ 調査対象国は、VMC取得時に必要なロゴの商標登録機関のある国から選定

BIMI普及に向けての課題 – 国内の低いDMARC普及率

Tomorrow, Together KDDI

JAPAN SMARTPHONE SECURITY ASSOCIATION

Googleの送信者ガイドラインへの対応などにより、DMARCの必要性が高まったことで、DMARC対応した企業は増加したが、その多くの企業ではDMARCポリシーが“none”となっている。BIMI対応するには、DMARCポリシーが”reject“ or ”quarantine”にする必要があり、DMARCポリシーの強化がネックになっている

DMARC実施のきっかけ

JP n=628

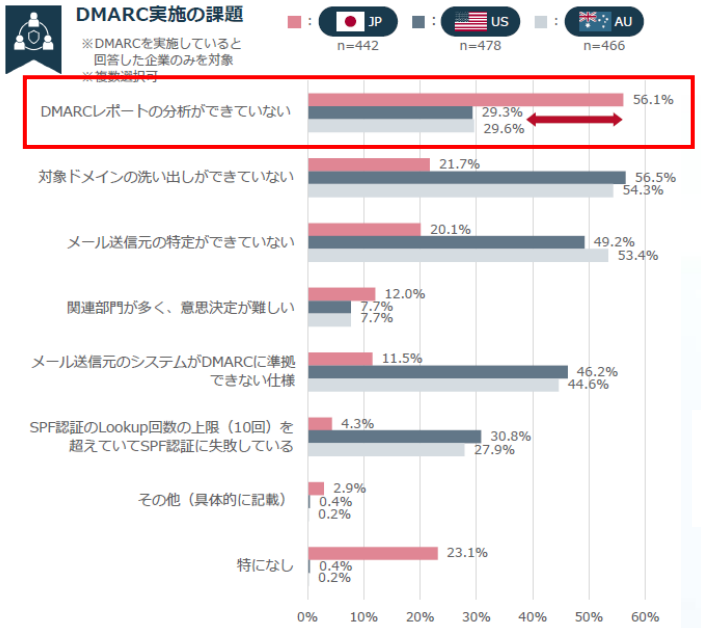
※ DMARCを実施・検討していると回答した企業のみを対象
※ 最大3つの複数選択可

1位	64.5%	Google（Gmail）の送信者ガイドラインへの対応
2位	50.8%	なりすましメールへの対策（セキュリティ対策強化）
3位	18.2%	自社ブランドの信頼性向上のため
4位	9.7%	取引先からの要請
5位	6.8%	関連省庁（経産省、警察庁、総務省）からの要請への対応
6位	2.5%	政府統一基準群への対応
7位	2.2%	その他（具体的に記載）
8位	1.8%	リスクレーティングサービス・診断からの指摘
9位	1.4%	PCIDSS v4.0への対応

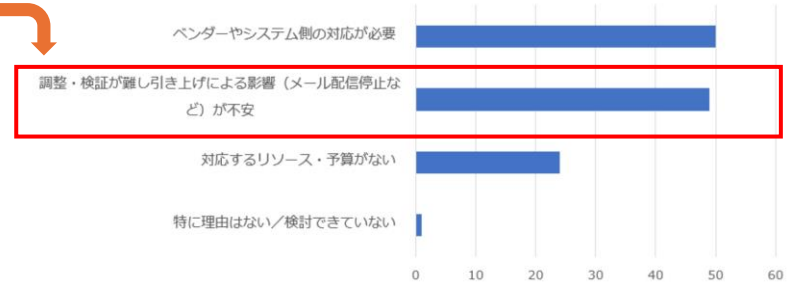
NRI Secure Insight 2024
https://www.nri-secure.co.jp/insight2024

DMARC実施の課題

※DMARCを実施していると回答した企業のみを対象
※複数選択可



DMARCポリシーの引き上げ（none→quarantine/reject）を行わない理由



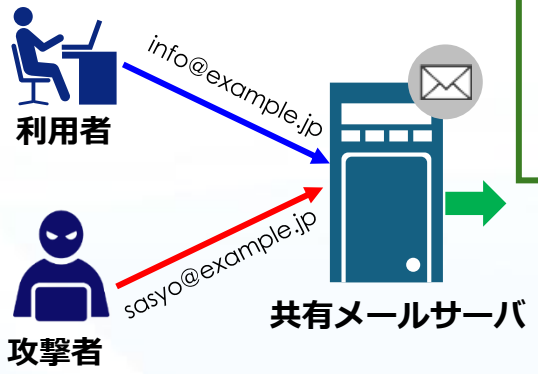
GMO BRABD SECURITY
企業ロゴ付きメール（BIMI)に関する長さ結果報告（対象者：メール配信者）
https://brandsecurity.gmo/news/post/post-20250902/

メールの到達を優先し、必要なセキュリティ対策が遅れる結果となっている

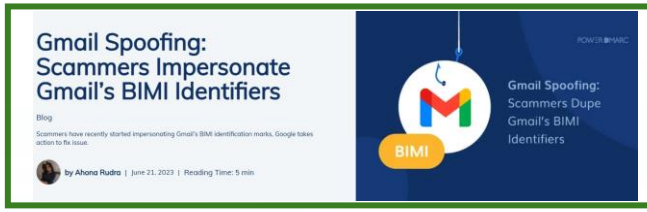
- 不正メールの排除やドメインの信頼性向上といった、**DMARCの本来の目的が達成されない**。
- メールの信頼性やブランド保護の効果が限定的となり、結果として**セキュリティリスクが残る**。

SPF=pass、DMARC=passフィッシング問題

20年以上前からメール送信時の**共有サーバ（共有IP）問題**（いわゆるお隣さん問題)として、IPを共有している場合、**なりすまし送信でSPF=pass**と出来る問題が指摘されてきた。さらにDAMRCが普及により、**DMARC=pass（SPF=pass、DKIM=none)**となるフィッシングメールが送信される事例も出ている。



攻撃者は、共有メールサーバに同居しているドメインを詐称してメールを送ることでDMARC/SPFを“pass”することが可能



Rudenberg discovered that Gmail's BIMI implementation only requires SPF to match. The DKIM signature can be from any domain.

https://powerdmarc.com/ja/gmail-bimi-logo-spoofing/

Domain-based Message Authentication, Reporting, and Conformance (DMARC)
draft-ietf-dmarc-dmarcbis-41

8. Conformance Requirements for Full DMARC Participation

This document describes the DMARC mechanism, and allows Domain Owners and Mail Receivers some leeway in deciding which parts of the mechanism to implement. This section summarizes the requirements for full participation in DMARC, either by Domain Owners or by Mail Receivers.

In order to fully participate in DMARC, Domain Owners:

✶ **MUST NOT rely solely on SPF for a DMARC pass if the DMARC policy for the Author Domain is "p=reject"**

受信サーバでは、**DMARCポリシーが“reject”の場合は、DMARC認証時にDKIMの認証を必須**とすることで、“reject”の価値が向上するのでは。また、送信側も共有IDのリスク回避のために、**SPFレコードは記載せず、DMARC-DKIM**のみで対応するなど発想の転換があってもよいのではと考えられる。

BIMI導入における課題 – DMARCポリシー問題

BIMIでは、BIMIのが要求する条件でDMARC認証をPassする必要があるが、親ドメインのDMARCポリシーが“none”になっていっているなど、BIMIが求める条件を満足しない状態でBIMIレコードを公開しているドメインが存在している。

BIMI適用時のDMARCの主な条件

- DMARCポリシーは **“quarantine”または“reject”**
- Heder Fromドメイン（RFC5322.From Domain）と**親ドメインの双方でDMARC対応**が必要
  - ✓ 親ドメインにDMARCの記述があればHeder Fromドメインにもポリシー適用される
- DAMRCのオプションパラメータのPCTを設定する場合は100（デフォルト値）とする必要がある
- DMARCのオプションパラメータの**SPを設定する場合は“quarantine”または“reject”**
- DMARC認証において、DKIM認証結果は“Pass”すること（**SPFのみ“Pass”は不可**）

ポリシーが”none“のドメイン数	ポリシーが“none”の企業数
91ドメイン	23企業
0.9%	1.8%

（ドメイン数 4,994、調査企業 2,565）

JSSECセキュリティコラム 「課題が残る送信ドメイン認証の導入・運用」
https://www.jssec.org/column/20250930.html

BIMI導入における課題 – 証明書の公開先

BIMIではVMC/CMCの証明書ファイル、表示するロゴデータ（SVG）をWebサーバ上に公開する必要がある。これらを公開するにあたっては、証明書発行会社のWebサーバ、SIerのWebサーバ、自社のWebサーバなどに公開するのが一般的である。この内、**自社のWebサーバに公開する場合、自社Webサーバの設定**によっては、証明書データ等の取得時に**問題が発生する場合**がある

【問題事例】

- 自社**Webサーバのメンテナンス**中に、証明書・ロゴの取得が不可となるケースがある
- WebサーバのMAX Cacheを“0”や“Non-Cache”にしているため、**メールbyメールで証明書・ロゴ取得が動作**し、サーバに過大な負荷が発生する
  - 認証情報をキャッシュさせたくないためなどの設定と想定される
- サーバのMAX Cache時間を**サーバ負荷軽減のため長く設定**している場合、キャッシュ保持中に証明書の有効期限が切れて認証失敗となる

証明書保存先

	Total	DigiCert	Entrust	GlobalSign
証明書発行先サーバ	60.2%	50.4%	86.7%	33.3%
上記以外	29.8%	49.6%	13.3%	66.7%

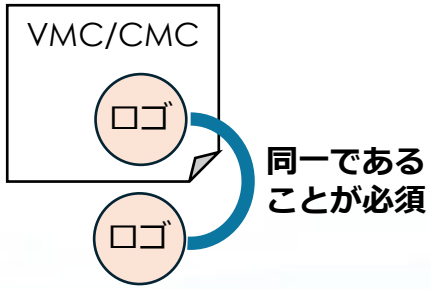
キャッシュ時間（証明書発行先Webサーバ以外）

設定なし	0秒	10 秒	1分以内	10分以内	1時間以内
64.8%	3.7%	0.1%	1.7%	8.8%	2.6%
1日以内	**1週間以内**	**1か月以内**	**半年以内**	**1年以内**	**1年以上**
2.0%	2.0%	2.8%	0.2%	10.6%	1.9%

JSSECセキュリティコラム 「課題が残る送信ドメイン認証の導入・運用」
https://www.jssec.org/column/20250930.html

BIMI導入における課題 – 仕様の曖昧さ

VMC/CMCの証明書にはロゴデータが含まれており、BIMI認証時には、**証明書内のロゴ**と**Webサーバに公開されているロゴ**が一致している必要がある。しかしながら、BIMI対応している一部のドメインでは、これらロゴが一致していないケースが散見される。



同一であることが必須

非公開

非公開

ロゴ不一致企業

39企業

JSSECセキュリティコラム 「課題が残る送信ドメイン認証の導入・運用」
https://www.jssec.org/column/20250930.html

Brand Indicators for Message Identification (BIMI)
7.9. Construct BIMI-Location URI
This header MUST NOT be added if Discovery or Validation steps failed.

If both a= and l= tags are included then the MTA MUST perform checks to ensure that the SVG Indicator referenced by the bimi-location is identical to the SVG Indicator extracted from the BIMI Evidence Document.

https://datatracker.ietf.org/doc/draft-brand-indicators-for-message-identification/

メールサービスによっては、**ロゴ表示されてしまう**ため、問題に気づかない可能性がある

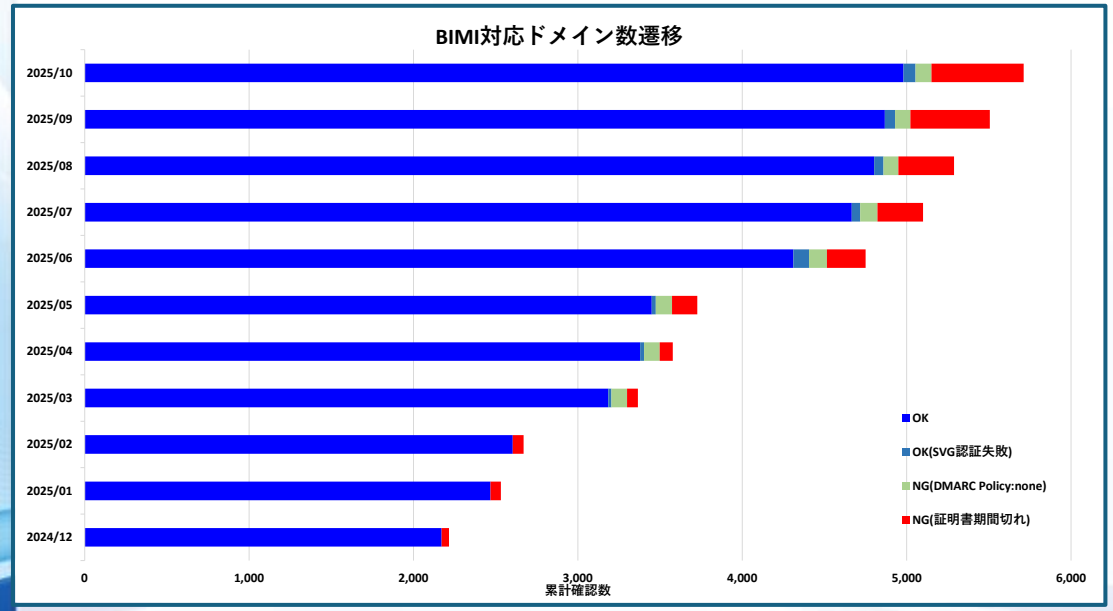
複数のメールサービスを使ってロゴ表示を**確認**することが重要

証明書内のロゴファイルは、証明書発行会社が厳格な審査を行い承認を行い、証明書に組み込んでいるため、証明書内のロゴデータとSVGロゴデータの検証を行う必要性があるかは疑問

BIMI導入における課題 – 証明書の更新漏れ？

VMC/CMCの証明書の有効期限は1年ですが、**更新漏れや証明書の差替忘れ**と推測される事象を確認している。

ロゴの認証の有効期限が切れているドメインが徐々に増えている。某ドメインでは、一定時間経過後、再度有効になった例も確認しており、なんらか理由で更新漏れやサーバの証明書の差替を忘れた可能性がある



※ JSSEC調べ

事例
2025/10/16で有効期限が切れたことでBIMI認証が失敗していたが、2025/10/20に証明書の更新がされたことで認証失敗が解消している。

Date: Thu, 16 Oct 2025 10:00:00 +0900
Authentication-Results: phl-mx-06.messagingengine.com;
bimi=pass header.d=**********.jp header.selector=default
policy.authority=pass policy.mark-type="Registered Mark"
policy.authority-uri=
https://vmc.digicert.com/0cf79468-3958-438d-8de0-**********.pem

Date: Mon, 20 Oct 2025 16:00:00 +0900
Authentication-Results: phl-mx-05.messagingengine.com;
bimi=fail (VMC has expired) policy.authority=fail
policy.mark-type="Registered Mark"
policy.authority-uri=
https://vmc.digicert.com/0cf79468-3958-438d-8de0-**********.pem

Date: Wed, 22 Oct 2025 10:00:00 +0900
Authentication-Results: phl-mx-08.messagingengine.com;
bimi=pass header.d=**********.jp header.selector=default
policy.authority=pass policy.mark-type="Registered Mark"
policy.authority-uri=
https://vmc.digicert.com/0cf79468-3958-438d-8de0-**********.pem

証明書の差替忘れを防ぐためには、証明書の公開先を**証明書発行会社のサーバ**で公開することが推奨される

BIMI導入時の利用者周知について

残念ながら、BIMIの認知はまだ広くないと推測されます。したがって、BIMI導入した際には、利用者にBIMIを使ったメールの安全な判別方法を周知することが推奨される。
新たにBIMI対応したサービス提供者は、周知方法は多種多様あると思われるが、利用者が理解できる方法での周知することを期待したい。

非公開

生成AIの脅威 ー フィッシングメールの高度化

生成AIによりフィッシングメールがより高度化することが想定され、利用者がより騙されやすくなることが推測されている。

- 人間らしい自然な文章作成可能になり、文章が洗練される。
  - ➢ **生成AIで何千・何万通りの試験を実施し、騙される可能性の高い攻撃**を行ってくる。
- 攻撃ターゲット（詐称するサービス）の公開情報やSNSなどの情報をタイムリーに学習させることで、**時事や個人に最適化したフィッシング**文面の作成が可能になる。
- ソーシャルエンジニアリングの高度化により、攻撃先（利用者）の情報を収集し、**個人の弱点や関心に合わせた説得力のある個別にカスタマイズした攻撃**が可能となる。
- **フェイクニュースの拡散と併せて攻撃**を行うことで、文章の**内容の信ぴょう性**を高めて攻撃を行う可能性がある。

生成AIによるサイバー攻撃が広まれば、利用者は真偽の判断をすることはより困難になり、生成AIを使ったセキュリティ対策も、負の生成AI vs 正の生成AIの対決となり、必ずしも期待できるとは言い難い

生成AI時代では、なりすましを識別することは出来ないと考え、正しい情報であることのみを識別することがリーズナブルである。

➡ **サイバー攻撃防御ではホワイトリスティングが優位**であり、**信頼性・真正性・完全性**が保証される、**BIMIの普及が重要**となる

BIMI/DMARCの安全性に向けての課題

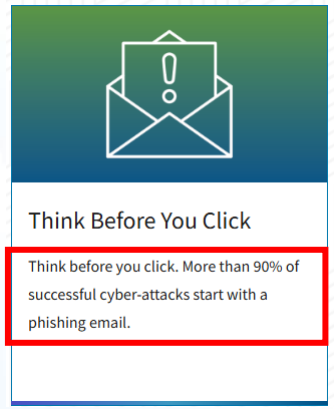
DAMRC/BIMIは送信メールの安全性が確保されてなりたつ技術である。一方、Scan Net Securityのインシデント・事故*では2025年だけで15件以上のメール乗っ取りによる不正メール送信の記事が掲載されている。また、アメリカ政府のセキュリティ機関であるCISAからは、サイバー攻撃の90%以上がフィッシングメールが起点となっていると説明している。これら背景から、メール送信するシステムのセキュリティ確保が重要となる。

*Scan Net Security インシデント・事故 https://scan.netsecurity.ne.jp/category/incident/

4 Things You Can Do To Keep Yourself Cyber Safe

Released: December 18, 2022

RELATED TOPICS: CYBERSECURITY BEST PRACTICES



https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

送信側の認証強化に向けて

INNOVATION > CYBERSECURITY

Stop Using Your Passwords—1Password And Google Warn

By Davey Winder, Senior Contributor. © Davey Winder is a veteran cybersecur... Follow Author

Published Nov 22, 2024, 07:22am EST

https://www.forbes.com/sites/daveywinder/2024/11/22/stop-using-your-passwords-1password-and-google-warn/

Google アカウントにログインするための最も簡単で最も安全な方法

パスキーはパスワードに代わるもので、パスワードよりも簡単かつ安全です。指紋認証、顔認証、または画面ロックだけで Google アカウントにログインできます。

https://www.google.com/account/about/passkeys/

Googleは認証の安全性確保のためパスキーの利用を強く推奨している

Exchange Online での基本認証の廃止

2024/06/25

基本認証は時代遅れの業界標準です。 当初、この機能を無効にすると発表して以来、脅威は増加の一途をたどっています （「セキュリティの向上 - 共に」 参照）。より優れた、より効果的なユーザー認証の代替手段があります。

POP、IMAP、および SMTP AUTH

2020 年に、POP、IMAP、および SMTP AUTH の OAuth 2.0 サポートをリリースしました。 一部のクライアント アプリへのUpdatesは、これらの認証の種類をサポートするように更新されています (たとえば、Thunderbird は、21Vianet によって運用Office 365を使用しているお客様向けではありません)、最新バージョンのユーザーは OAuth を使用するように構成を変更できます。 OUTLOOK クライアントが POP と IMAP の OAuth をサポートする予定はありませんが、Outlook は MAPI/HTTP (Windows クライアント) と EWS (Outlook for Mac) を使用して接続できます。

https://learn.microsoft.com/ja-jp/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online#pop-imap-and-smtp-auth

Microsoftも基本認証を廃止し、OAUTHを使った認証の利用を進めている

BIMI/DMARCが安心して利用できるようにするには、メール送信側のセキュリティ確保が不可欠であり、企業やB to Cのメールを送信するシステムでは**より強度な認証の採用**が推奨される

まとめ

- セキュリティ対策は、**利用者が容易に理解できて使える**ものである必要がある。その意味で、BIMIは口ゴの表示の有無によって、その**メールの安全性を直感的に理解できる**対策と言える。
- BIMIは、**真正性・信頼性・完全性が担保**されたメールのセキュリティ対策として、現時点では非常に有効な手法の一つと考えられる。
- また、BIMIにはセキュリティ面だけでなく、**ブランド価値の向上**といった効果も期待できる。
- ただし、どんなセキュリティ対策も、**正しく運用**されなければ意味がない。BIMIを導入する際は、その設定が適切かどうかを継続的に確認し続けることが重要。
- さらに、いかに有効な対策であっても、それが広く普及しなければ十分な効果は得られない。そのため、BIMIの有効性を最大化するためには、**より多くのサービス提供者やメール運用者がBIMIに対応していくことが期待**される。
- メール送信側は、アカウントの乗っ取りリスクを最小限に抑えるために、**より強固な認証技術を採用すべき**である。これにより、DMARC/BIMIの効果も最大化され、安全なメール環境を実現できる。

講演内容の解説について2025年11月末のJSSEC25年11月号セキュリティコラムで公開予定です。

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC

https://www.jssec.org