各　位

2024年9月4日
サイバネットシステム株式会社

フィッシング脅威が拡大する中、自社を装うなりすましメールを防ぐ
－DMARC/BIMI 運用自動化ソリューション－「Valimail」販売開始のお知らせ

導入が急務とされるDMARCの設定から運用までを自動化。
運用コスト削減と強固なフィッシングメール対策の両立を実現します。

サイバネットシステム株式会社（本社：東京都、代表取締役 社長執行役員：白石 善治、以下「サイバネット」）は、Valimail Inc.（バリメイル・インク、本社：米国コロラド州、以下「Valimail社」）と販売代理店契約を締結し、同社が開発した「Valimail（バリメイル）」の販売を2024年9月4日より開始したことをお知らせします。

フィッシングメールによるサイバー攻撃の増加により、DMARC対応が急務に

近年、電子メールを介して個人情報や金融情報を搾取するフィッシングによるサイバー攻撃が爆発的に増加しています。警視庁の発表資料によると、2023年度に国内で報告されたフィッシング件数は初めて100万件を超え、過去最多の1,196,390件（前年比23.5%増加）記録しました※1。

こうしたフィッシングメールに有効な対策とされる送信ドメイン認証DMARC※2は、ドメインの改ざんや「なりすまし」を検知できる技術として欧米諸国を中心に普及が進んでいます。国内においても、大手メールサービスの提供元や政府機関をはじめ、さまざまな業界でフィッシング対策強化の重要性が認識され、対応要請が急速に進んでいます。

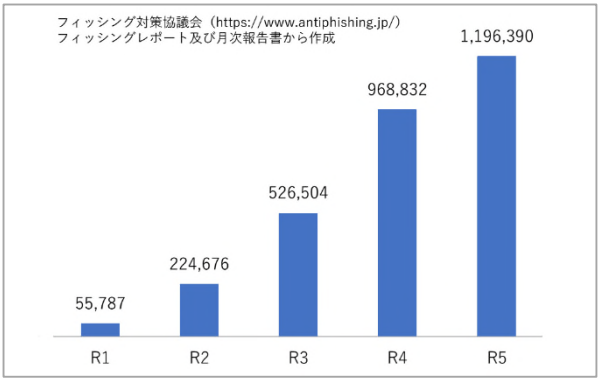

図１：フィッシング報告件数の推移（警視庁発表資料「令和５年におけるサイバー空間をめぐる脅威の情勢等について」※1より）

対象業界	要請元	要請内容
一定量のメール送信企業	大手メールサービス Gmail（米Google LLC提供）、Yahoo! Mail（米Altaba Inc.）、iCloudメール（米Apple Inc.提供）など	＜要請内容例＞**「Gmailガイドライン」**※3 2024年2月より、「Gmail」宛てに１日5,000通以上の電子メールを配信する組織は、SPF、DKIM、DMARC対応が義務付け
クレジットカード会社	経済産業省、警察庁、総務省	2023年2月にフィッシング対策強化の一環として、クレジットカード会社へのDMARC対応を要請※4
政府／自治体等	内閣サイバーセキュリティセンター（NISC）	政府統一基準（2023年7月改訂）※5において、DMARC対応が要件に含まれる
流通／小売り企業等	クレジットカード会社	カード情報セキュリティの国際統一基準であるPCI DSS v4.0※6において、カード情報を扱う企業に対し2025年3月までにDMARC対応を要請

図２：DMARC対応が求められる業界例

DMARC 未導入の企業が直面するリスク

自社のメールサーバがDMARCに対応していない場合のリスクは、すでに対応済みの宛先へ送信したメールがスパムメールとして処理されることにとどまりません。自社ドメインが悪用され、フィッシング詐欺につながる「なりすましメール」が配信されることで取引先が被害を受けるような場合、ドメインの封鎖に追い込まれたり、相手企業から損害賠償を求められたりするリスクも考慮する必要があります。今後、DMARC対応による顧客・取引先などのサプライチェーン保護は、必須と言えます。

サイバネットシステム株式会社 〒101-0022　東京都千代田区神田練塀町３　https://www.cybernet.co.jp/

DMARC/BIMI 運用自動化ソリューション「Valimail」とは

DMARCの導入と適切な運用には、技術的な専門知識が必要です。また、「DMARCポリシー」※7を強化し、高いセキュリティ水準を維持していくためには、継続的なメンテナンスが不可欠です。

DMARC/BIMI運用自動化ソリューション「Valimail」は、DMARCの運用を自動化するサービスで、ユーザーの専門知識の有無にかかわらず、迅速かつ効果的なDMARC運用を可能にします。

DMARC認証に失敗したメールの処理方法を設定した「DMARCポリシー」を、最も強化された「Rejectレベル」へ移行するには、専門の技術者でも通常半年～1年間かかるとされています。「Valimail」の自動化ツールを利用すれば、専門知識はなくとも期間を大幅に短縮することが可能です※8。

「Valimail」は、DMARC技術に関連する約18件の特許を有し、DMARC運用の自動化に特化したプラットフォームとして世界中で5万社以上の企業に導入され、その技術力と信頼性が認められています。

「Valimail」の特長

- **DMARCの設定から運用までを自動化することで、手間とコストを大幅に削減！**
  DMARCポリシーの適用、リアルタイムモニタリング、異常検知時のアラート通知などの機能が提供されるため、専門知識がなくても簡単に高品質なセキュリティ対策を実現します。

- **認証状況を詳細に分析し、セキュリティ状態を可視化！**
  認証成功率や失敗率、なりすましメールの検出などのデータが定期的にレポートとして提供されるため、企業はセキュリティ体制の強化に必要なデータを容易に取得し、改善すべき点を把握することができます。

- **BIMI※9自動設定による自社ブランドロゴの付与で、信頼性を強化！**
  DMARC認証と連携したBIMI自動設定が可能なため、正規のメールに自社のブランドロゴを表示し、安全であることを可視化して受信者に信頼性をアピールすることができます。これによってブランドの信頼性も強化でき、メールの開封率の向上にもつながります。

Valimailの詳細については、下記Webサイトをご覧ください。
https://www.cybernet.co.jp/valimail/

Valimail社からのコメント

Valimail CEO 兼共同創設者
Alexander Garcia-Tobar 氏

近年、日本政府や米Google社からのDMARC導入要請などが相次ぎ、Valimailのサービスが日本のお客様に、今まさに必要とされるタイミングだと感じています。実際に、私たちのDMARC自動化サービスを導入する日本の企業は急増しています。

また、日本は私にとって家族や過去の仕事の経験から特別な思い入れのある場所です。そのため、サイバネットをはじめとする日本のパートナーを通じ、この地でValimailの事業を拡大できることを、大変嬉しく、光栄に思っています。

サイバネットのセキュリティソリューション

サイバネットは、1998年より企業向けセキュリティソリューションの取り扱いを開始して以来、最先端のセキュリティソリューションやサービスを提供してまいりました。

国内で急務となっているDMARC対応およびメールセキュリティ強化のニーズに応えるため、ValimailのDMARC/BIMI

運用自動化ソリューションとサイバネットのセキュリティソリューション提供力を組み合わせ、包括的なセキュリティソリューション対策を提供していきます。

サイバネットのセキュリティソリューション詳細については、下記Webサイトをご覧ください。
https://www.cybernet.co.jp/itsolution/

注釈

※１： 出典：警視庁発表資料「令和５年におけるサイバー空間をめぐる脅威の情勢等について」２頁（令和6年3月14日公開）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

※２： DMARC（Domain-based Message Authentication, Reporting and Conformance）：電子メールにおける送信ドメイン認証技術の一つ。ドメインの改ざんやなりすましを防ぎ、事前に設定したポリシーに従って処理するための仕組み。

※３： 出典：Google社による管理者向けサポート「メール送信者のガイドライン」
https://support.google.com/a/answer/81126?visit_id=638553918928535986-2543878000&rd=1

※４： 出典：経済産業省・警察庁・総務省発表のニュースリリース「クレジットカード会社等に対するフィッシング対策の強化を要請しました」（2023年2月1日公開）
https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

※５： 出典：内閣官房 内閣サイバーセキュリティセンター発表資料「政府機関等の対策基準策定のためのガイドライン」（令和5年7月4日公開）320頁
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

※６： 出典：PCI Security Standards Council, LLC提供資料「Payment Card Industryデータセキュリティ基準：要件とテスト手順」v4.0（2022年3月）154頁
https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0-JA.pdf

※７： DMARCポリシー：DMARC認証に失敗したメール処理方法を決める３種類の設定。処理方法が緩めなものから順に、１.None（監視のみ）、2. Quarantine（隔離）、3. Reject（拒否）。最初の導入時は「1. None」で設定し、最終的には「3. Reject」へと段階的に強化させることが推奨されている。

※８： 出典：Valimailの製品説明
https://www.valimail.com/why-valimail/

※９： BIMI（Brand Indicators for Message Identification）：DMARC認証が成功したメールに対し企業ロゴを付与し信頼性を高める技術。

Valimail社について

Valimail Inc.は、2015年に設立され、メールセキュリティと認証技術のリーディングカンパニーとして成長しました。設立当初から、企業のメールセキュリティを向上させるために、自動化技術を駆使した革新的なサービスを提供してきました。現在、グローバルで5万社以上の企業に導入され、その顧客には政府機関、金融機関、製造業、IT、メディアなどが含まれ、多様な業界で高い評価を受けています。また、フォーチュン500企業の多くがValimailを採用しており、その技術力と信頼性が認められています。

Valimail社に関する詳しい情報については、下記Webサイトをご覧ください。
https://www.valimail.com/

サイバネットについて

1985年の創業以来、物理学などの科学技術とデジタル技術の両面に精通した技術者集団として、製造業の研究・開発・設計部門や大学・政府の研究機関を中心に、コンピュータシミュレーションやサイバーセキュリティ、AR/VR、医用画像処理などに関わるデジタルソリューションおよび技術コンサルティングサービスを提供しています。

近年は、CAE、MBD、MBSEを中心とした製造業におけるエンジニアリングチェーンの革新に加え、PLMやIoTを活用したサプライチェーンの高度化に関わる分野にもソリューションの提供範囲を拡大しています。また、サイバーセキュリティ分野では、最新の脅威に対応した先端的なソリューションを複合的に提供できる体制を構築してきました。さらに、AIを活用したプログラム医療機器の分野において国内で初めての医療機器承認ならびに公的医療保険の適用を受けるなど、医療AIのパイオニアとして業界をリードしています。

サイバネットシステム株式会社に関する詳しい情報については、下記Webサイトをご覧ください。
https://www.cybernet.co.jp/

本件に関するお問い合わせ先：**サイバネットシステム株式会社**

内容について：
ITソリューション事業部　営業部
担当：中西
E-MAIL：itdsales@cybernet.co.jp

報道の方は：
コーポレートマーケティング室
担当：宮本
E-MAIL：prdreq@cybernet.co.jp

サイバネットシステム株式会社 〒101-0022　東京都千代田区神田練塀町３　https://www.cybernet.co.jp/