ドメイン名動向ハイライト：2023年10月

WhoisXML APIの研究者がこのほど、2023年10月に新規登録された数百万のドメイン名から無作為に31,000個を抽出し、WHOISデータ、登録者の国、レジストラ、TLDの共通点を調べました。

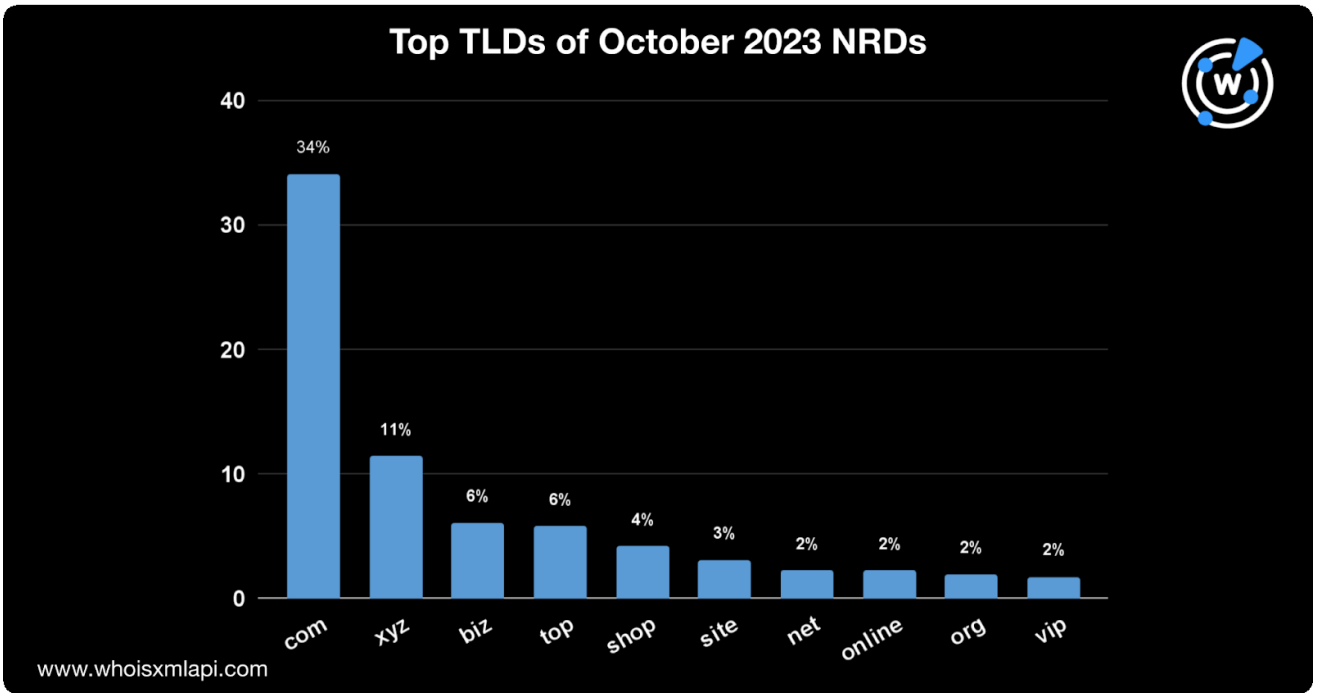
また、ドメイン名の文字列の使用状況を分析して新たな潜在的傾向を明らかにするとともに、予測インテリジェンスソースを活用して10月に最も模倣されたブランドや文字列を特定しました。本調査の結果と、DNS、IPアドレスおよびドメイン名のインテリジェンスを用いてWhoisXML APIが作成した脅威レポートへのリンクを以下に示します。

10月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

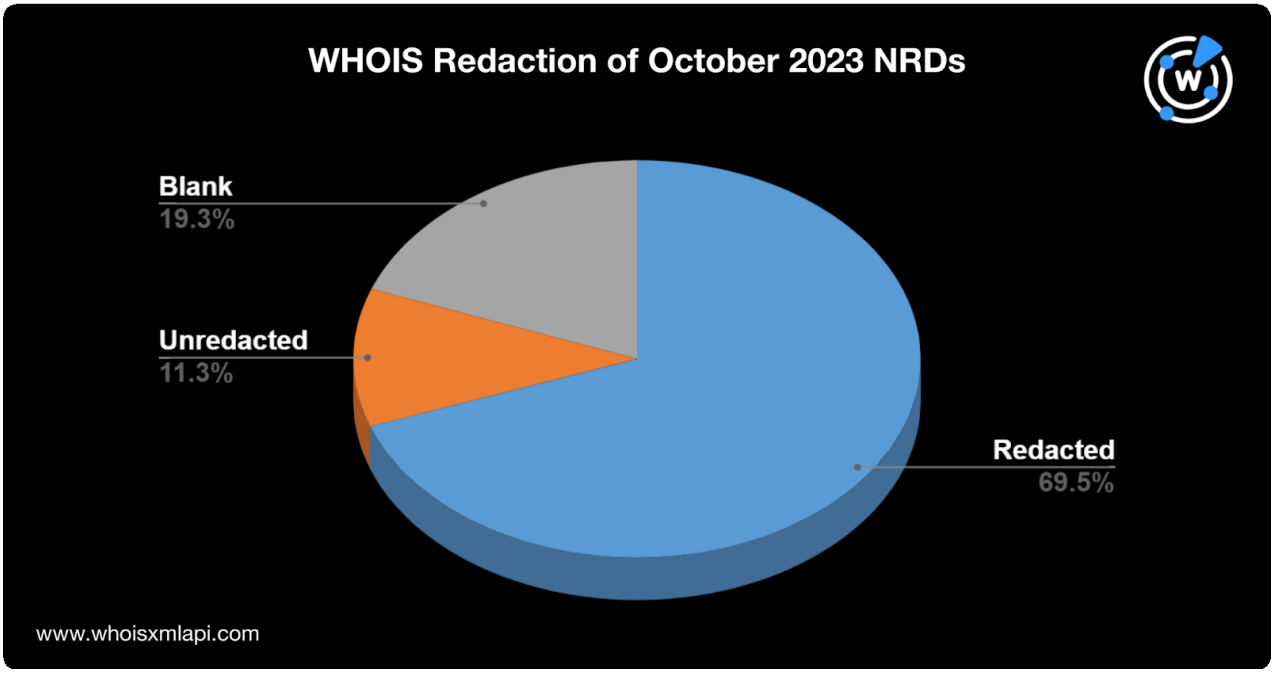
2023年10月のTLDトップ10は前月とほぼ同じでした。最も人気があったのは.comで、NRD登録数全体の34%を占めました。2位から10位は、.xyz（11%）、.biz（6%）、.top（6%）、.shop （4%）、.site（3%）、.net（2%）、.online（2%）、.org（2%）、.vip（2%）となりました。

NRDの73%は上位10 TLDのドメイン名でした。残りは630を超える他のTLDに分散しています。

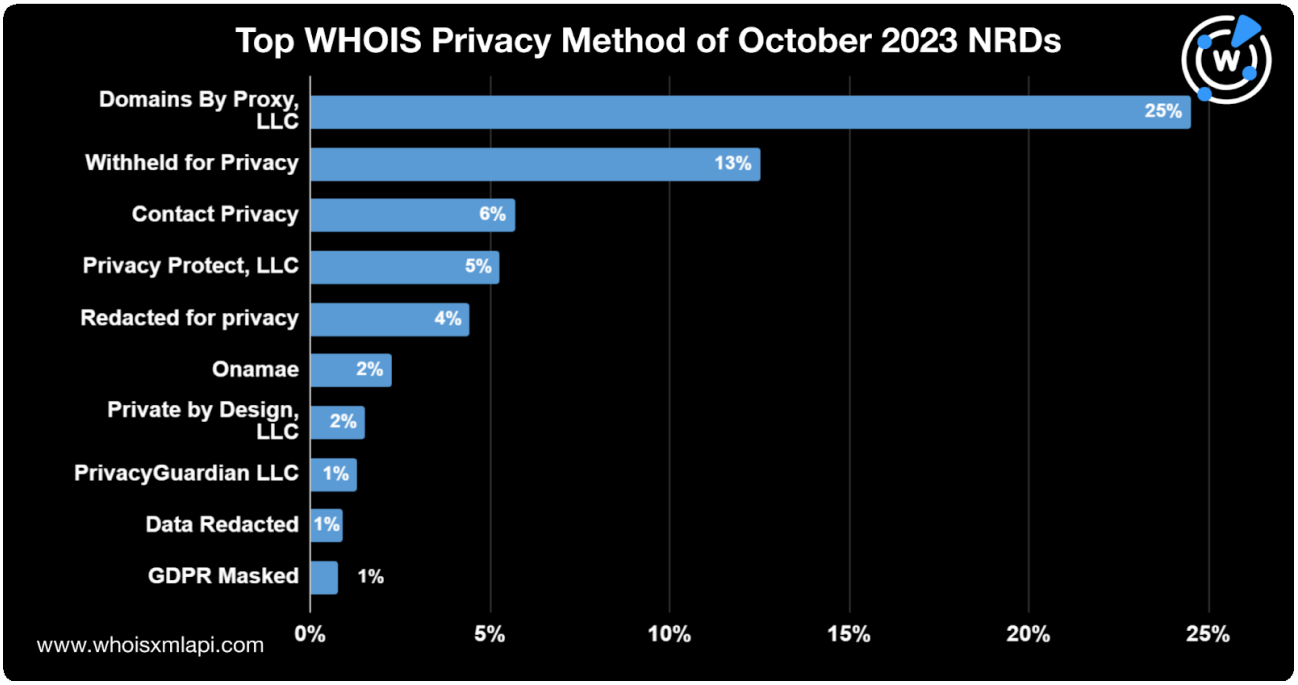


WHOISデータの非公開化

NRDのうち約70%では、WHOISレコードが編集されて非公開に、つまり登録者の身元がわからない状態になっていました。登録者の組織名が公開されていたのはわずか11%ほどで、約19%はそのフィールドが空白でした。



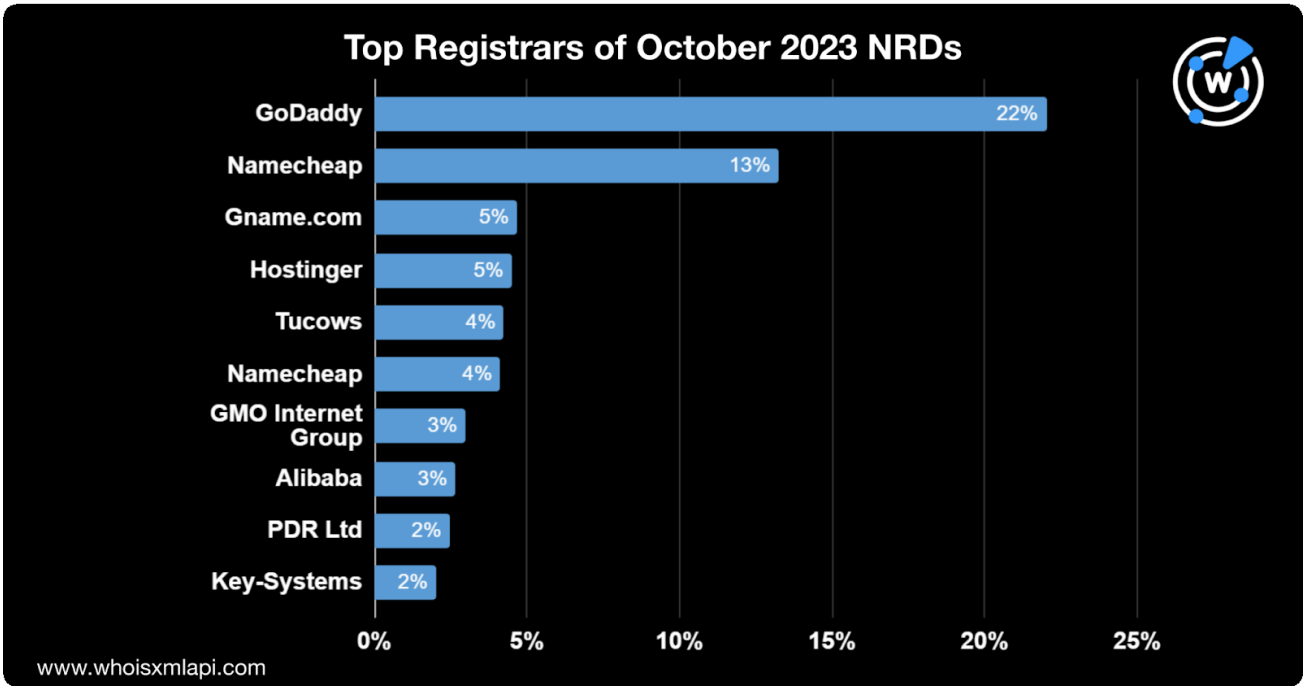
最も人気のあったプライバシーサービスプロバイダーはDomains By Proxyで、NRDの4分の1で使われていました。次いで多かったのはWithheld for Privacy（13%）、Contact Privacy（6%)、Privacy Protect（5%）、お名前（2%）、Private by Design（2%）、Privacy Guardian（1%）でした。



複数の登録者が、WHOISの登録者組織名欄に**Redacted for privacy**、**Data Redacted**、**GDPR Masked**などと表示していました。

レジストラの分布

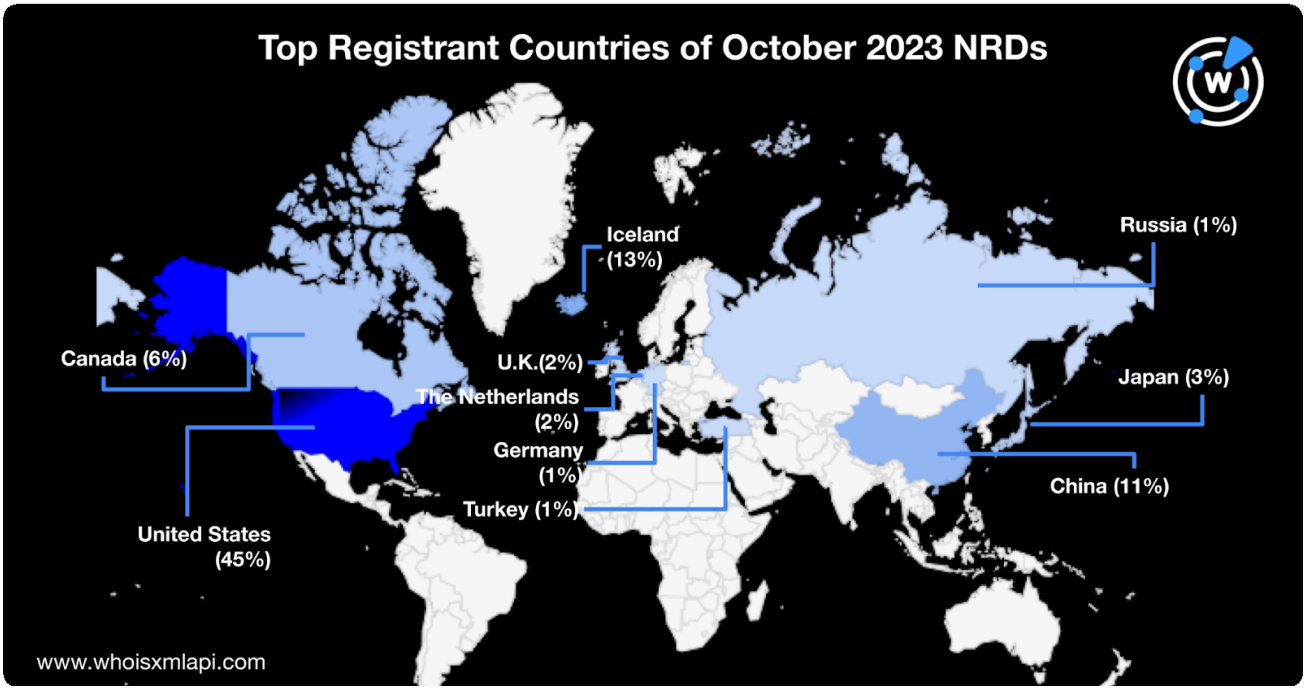
最も人気のあったドメインレジストラはGoDaddyで、NRDのうち22%を管理していました。次いで多かったのは、Namecheap（13%）、Gname（5%）、Hostinger（5%）、Tucows（4%）、GMOインターネットグループ（3%）、Alibaba（3%）、PDR Ltd.（2%）、Key-Systems（2%）でした。



トップ10のレジストラが総NRD数の63%を管理していました。残りの37%のNRDは、他の350を超えるレジストラに分散しています。

登録数上位の国

ドメイン名の新規登録が最も多く行われた国は米国で、全体の45%を占めました。2位と3位はアイスランド（13%）と中国（11%）でした。トップ10の4位以下は、カナダ（6%）、日本（3%）、英国（2%）、オランダ（2%）、ロシア（1%）、トルコ（1%）、ドイツ（1%）となりました。

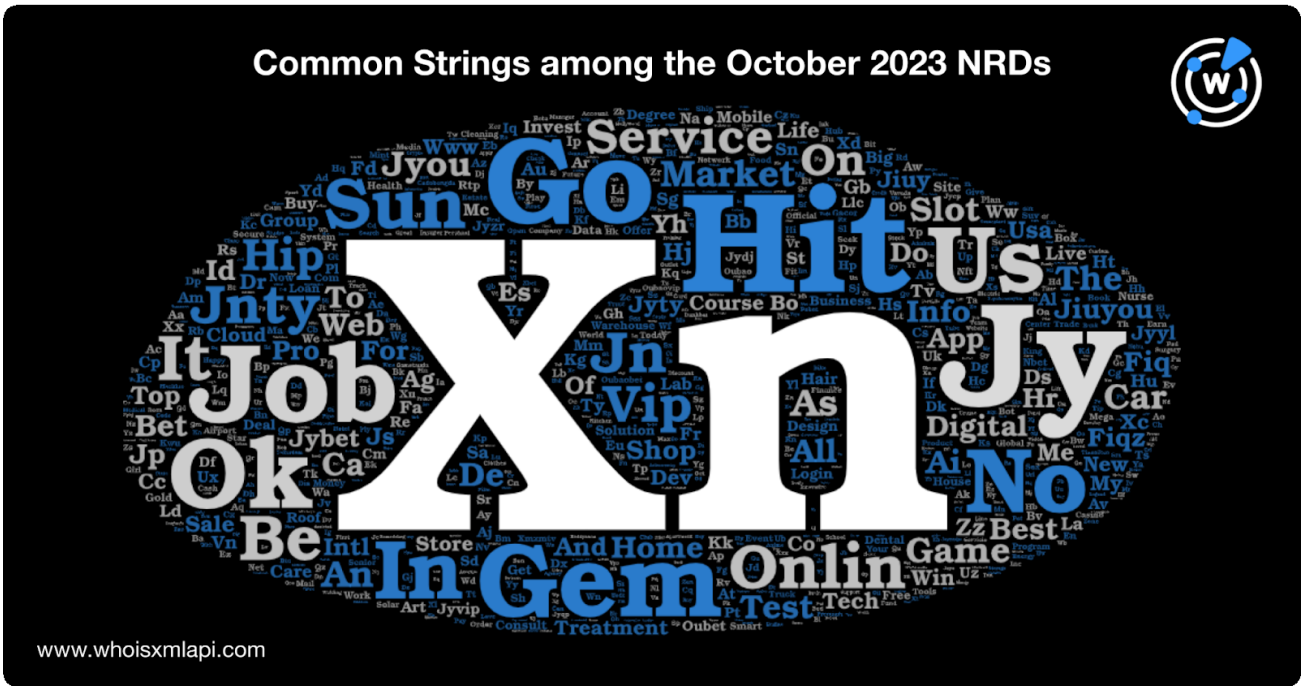


登録者数上位10カ国が総登録数の85 %を占めました。残りの15%は130を超える他の国に分散しています。

第2レベルドメイン（SLD）に共通して見られる文字列

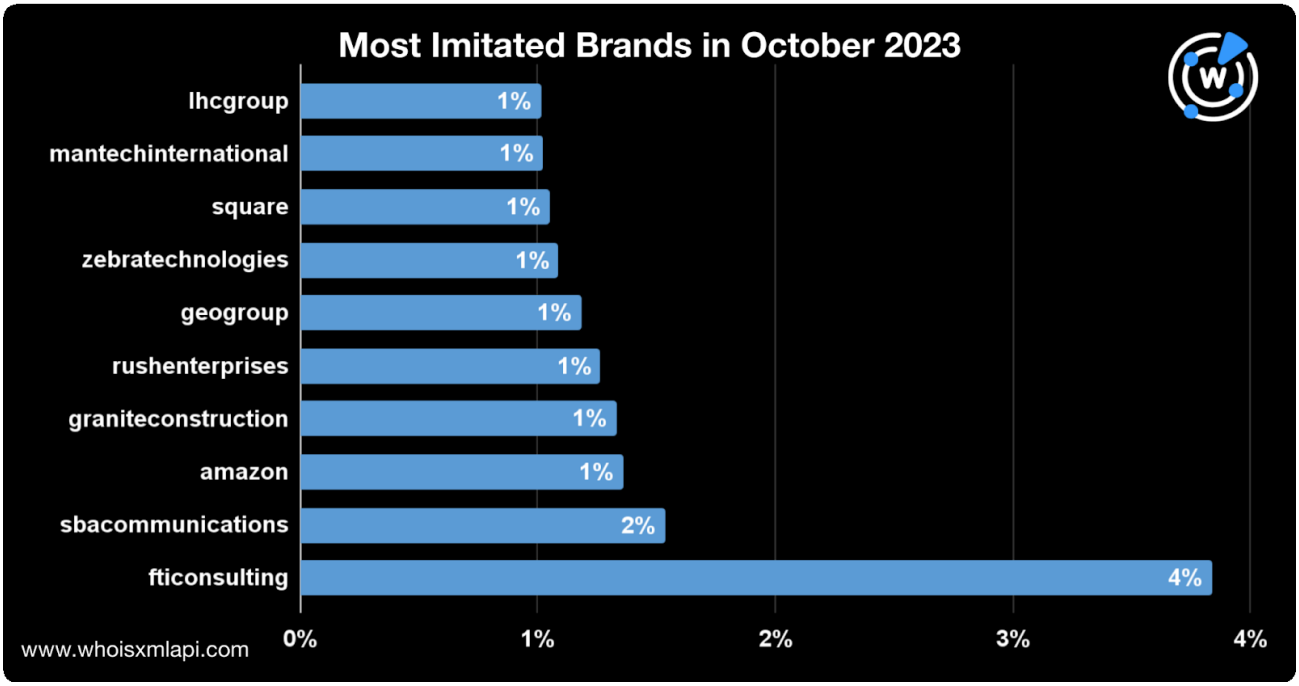
10月にNRDの文字列として最も多く見られた単語は、インターネットに関連するものでした。例えば、**service**、**online**、**test**および**shop**です。**go**、**hit**、**job**、**market**、**gem**、**game**もよく使われていました。

また、依然として**xn**がよく見られ、国際化ドメイン名（IDN）が引き続き登録されていることを示唆していました。



Early Warning Phishing Feedによるフィッシングの早期検出

Early Warning Phishing Feedのサンプルとして数千のドメイン名を抽出、分析したところ、最も頻繁に出現した文字列は**fticonsulting**で、不審なドメイン名のほぼ**4%**に含まれていました。他によく見られた文字列としては、**sbacommunications**、**amazon**、**graniteconstruction**、**rushenterprises**、**geogroup**、**zebratechnologies**、**square**、**mantechinternational**および**lhcgroup**がありました。



DNSのレンズで見るサイバーセキュリティ

当社が10月に公開した脅威リサーチ報告の一部を以下にご紹介します。

- **.topドメインを悪用するフィッシンググループを発見**：当社の脅威リサーチャーであるDancho Danchevが.topドメインを悪用するフィッシングを発見し、さらに当社の研究チームが4,000以上の関連アーティファクトを発見しました。

- **QRコードフィッシングの痕跡をDNSで探す**： QRフィッシングコードキャンペーンに関連するセキュリティ侵害インジケーター（IoC）として特定された18個のURLをもとに、WHOISとDNSのインテリジェンスを駆使して10,000超の関連アーティファクトを特定しました。

- **DNSでMessengerフィッシングの足跡をキャッチ**：パスワードを窃取するマルウェアを使ってFacebookのビジネスアカウントを標的に活動しているフィッシングキャ

ンペーン「MrTonyScam」を当社で調査しました。そして、攻撃者がDNSに残した痕跡から、10件を超える公開メールアドレスと、脅威のIoCと同じメールアドレスや文字列を共用している合計1,000超のアーティファクトを特定しました。

当社の過去の脅威レポートはこちらでご覧になれます。

今回のドメイン登録の分析や他のユースケースのサポートで使用した当社の商品につきましては、こちらまでお気軽にお問い合わせください。