メッセージングテクノロジー
なりすましメール対策としてのDMARCの普及

1.1 はじめに

ここでは、迷惑メールを中心としたメールの動向と、迷惑メール対策に関係する技術動向について報告します。

2008年の創刊以来、迷惑メール量の変化を示す指標として、IIJのメールサービスで検知した迷惑メールの受信メールに対する割合の推移を報告してきましたが、本年度からのメールシステムのリニューアルに伴い、これまでの形式での報告は今回が最後となります。今後は、大きな変化や動きなどがあった場合に、別の形で報告します。

技術動向は、引き続き送信ドメイン認証技術の解説や普及状況を報告します。また、送信ドメイン認証技術DMARCの導入に関して、昨年、法的な整理がなされましたので、その概要についても報告します。

1.2 迷惑メールの動向

迷惑メールの動向を示す指標として、ここではIIJのメールサービスが提供する迷惑メールフィルタで検知した迷惑メールの割合の推移を報告します。今回は、これまでの調査結果全体について、2008年の第23週（2008年6月2日からの1週間）から2017年の第52週（2017年12月25日からの1週間）までの期間、ちょうど500週分の推移となります（図-1）。

2017年の迷惑メールの割合の平均は30.5%でした。2016年の平均が39.9%でしたので、9.4%減少したことになりますが、2015年は平均24.7%でしたので、単純に減っているわけではなさそうです。実際に迷惑メールの中には、引き続き大手企業を詐称したフィッシングメールが現在も多く存在しますし、最近ではランサムウェアの実行に導くような悪質な迷惑メールも増えているようです。

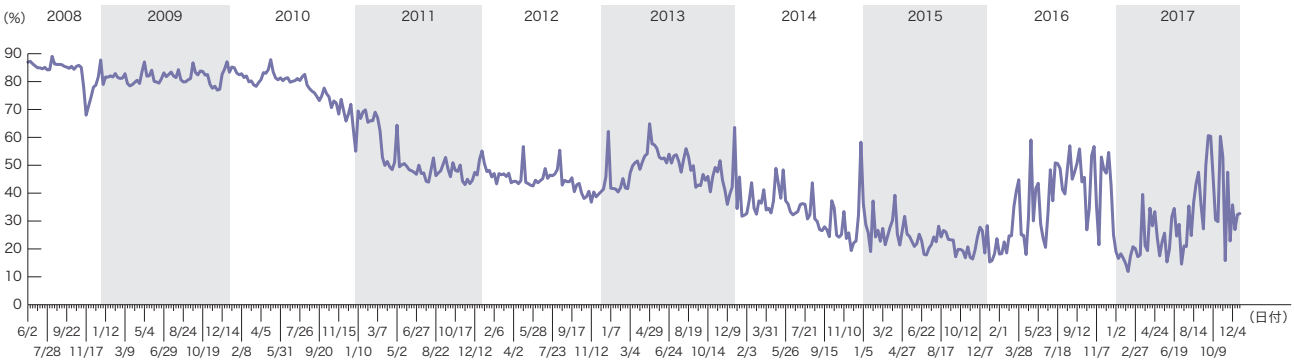

図-1 迷惑メール割合の推移

1.2.1 フィッシングメールの認証結果

前回(Vol.35)は、マイクロソフト社を詐称する迷惑メールについて、その送信ドメインの認証結果を報告しました。その後も大手企業を詐称するメールが続いています。

フィッシング対策協議会では、フィッシングメールの情報を公開[*1]していますので、届いたメールに示されたURLやHTMLファイルを開く前に、最近流通しているフィッシングメールかどうかを確認することが大切です。しかし、送信ドメイン認証技術を利用することで、もっと簡単にフィッシングメールを見破る方法があります。大手企業の多くは、既にDMARCを導入していますので、DMARC認証をすることで送信者情報が詐称されているかを判断できます。

Apple社を例に取ると、iCloudへのログインに関するメールに対しては、SPF、DKIM、DMARCすべてに対応したメールを送信します。最近送信されているフィッシングメール(図-2)では、メールヘッダ上の送信者情報(RFC5322.From)に本物と同じドメイン名email.apple.comを利用します。当然のことながら、送信元が違いますのでSPFは失敗(softfail)しますし、DKIMの署名はない(none)ので、DMARCの認証は失敗(fail)することになります。しかも、email.apple.comのDMARCレコードは、ポリシーがreject(p=reject)ですので、DMARCの仕様に沿った受信判断をする場合、こうしたメールは届かないことになります。

「楽天市場」や「楽天カード」を詐称したメールも依然として数多く送信されています。同様にこれらもヘッダ上の送信者情報にrakuten.co.jpやmail.rakuten-card.co.jpドメイン名を利用していますが、いずれのドメイン名もDMARCレコードを設定しています。そのため、すべてDMARC認証が失敗していますので、簡単に詐称メールと見破ることができます。送信ドメインのDMARC導入が進めば、こうした不要なメールを排除できるようになります。また、詐称されやすいドメイン名を管理している場合は、詐称対策としてのDMARCレコードの設定が望まれます。


お客様のApple ID が、ウェブブラウザからiCloudへのサインインに使用されました。

日付と時間：2018年3月8日 22:08 JST

のブラウザ： Chrome

オペレーティングシステム： Windows

IP：[redacted]

上記が問題でない場合は、このメールを無視してください。

最近iCloudへサインインを行ったことがなく、他者が違法にお客様のアカウントを使用していると考えられる場合は、Apple IDでパスワードをリセットしてください。

今後ともよろしくお願い致します。

Apple サポートセンター

Apple ID | サポート | プライバシーポリシー
Copyright 2018
Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.
すべての権利を保有しております。

図-2 Apple社を詐称するメール

＊1　フィッシング協議会：フィッシングに関するニュース(http://www.antiphishing.jp/news/alert/)。

1.2.2 メールの新たな脅威

米国FBIのIC3（Internet Crime Complaint Center）は、2017年のInternet Crime Reportを発表[*2]しました。その中の2017年のトピックスとして挙げられているものに、BEC[*3]とランサムウェア（Ransomware）があります。

BECは、巧妙な手口でメール受信者を騙して不正送金させる詐欺行為の1つです。IC3では、2017年に15,690件の苦情を受け、6.75億ドル以上の損失が発生したと報告しています。

日本でも大手航空会社が2017年9月に取引先を装った送金先変更のメールに騙され、3億円以上の被害が発生したことを同年の12月に公表し、大きなニュースとなりました。もちろん、多くのメール利用者は、こうした詐欺メールに騙されるわけがないと考えているかもしれません。しかしながら、実際には多くの被害が発生していますし、報道などによればかなり巧妙な手口を使って用意周到に準備した上で実行しているようです。被害に遭わないためにも、まずは技術的な対策をしっかり導入することが必要でしょう。

日本でも2017年5月に大きなニュースとなったWannaCryはランサムウェアであり、広義には不正プログラム（マルウェア）の一種となります。ランサムウェアに感染すると、重要なファイルが暗号化され、解読する鍵を得るために仮想通貨などでの支払いを要求されます。感染経路は様々ですが、そのひとつに標的型攻撃も含まれますので、メールの対策も重要となります。これまでのマルウェアのビジネスモデル（機密情報などを入手し別途闇市場などで金銭を得る）と異なり、被害者から直接金銭を得る手法であること、送金手法として仮想通貨を要求することで受け取り手の実態を掴めなくする、といった手法が新しいと言えます。

IC3では、2017年にランサムウェアと認識できた苦情が1,783件、被害額が230万ドル以上と報告しています。今年に入ってからも、3月に米国アトランタ市でランサムウェアの攻撃を受け、大きな被害が発生しているようです[*4]。

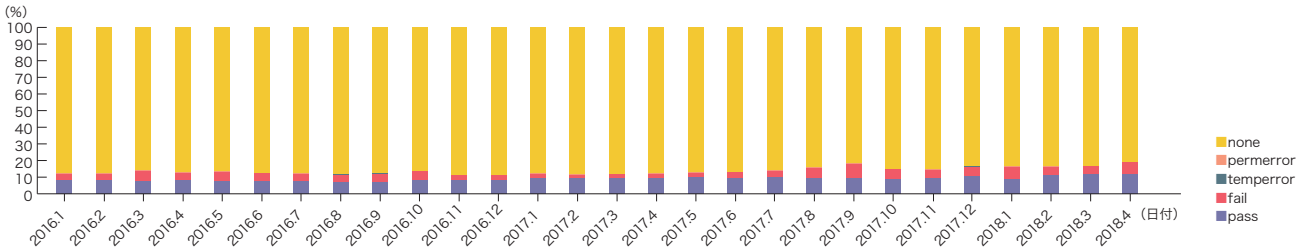

図-3 DMARC認証結果の推移

＊2　FBI、"Latest Internet Crime Report Released"（https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718）。
＊3　BEC：Business Email Compromise。
＊4　The City of Atlanta、"Ransomware Cyberattack Information"（https://www.atlantaga.gov/government/ransomware-cyberattack-information）。

1.3 メールの技術動向

ここでは、送信ドメイン認証技術DMARCの普及状況や関連技術も併せた標準化動向、日本で導入する場合に重要となる法的な取り扱いについて報告します。

1.3.1 DMARCの普及状況

IIJのメールサービスでは、受信したメールに対してDMARC認証を実施しています。DMARCの認証結果の2018年4月までの毎月の平均の推移を図-3に示します。

最新の調査結果である2018年4月の受信メールでは、DMARC認証できたメールの割合が、これまでの調査で最も高い割合の19.3%となりました。認証結果がpassであった割合も最も高く、12.2%という結果でした。まだDMARCが普及しているとは言えないレベルですが、少しずつDMARCを導入するドメイン名が増えています。

次に、SPF、DKIMを含めた送信ドメイン認証技術の認証結果のうち、2018年4月の組み合わせを図-4に示します。図-4の"DMARC+SPF+DKIM"の項目(8.8%)は、DMARCとSPFとDKIMすべての認証がpassした割合を示しています。つまり、DMARC認証できたドメイン名で最も多い組み合わせは、SPFもDKIMも導入しているドメインであることが分かりました。これは前回の調査結果(Vol.35)と同じ組み合わせでした。認証の組み合わせで最も割合が高いのは、"SPF"単体(35.4%)でした。他との組み合わせを含めて"SPF"でpassした割合の合計は69.3%となり、やはり導入の容易さが普及の要因であることが推測できます。総務省の最新の取りまとめデータ[*5]の2018年3月では、passの割合が90%を超えていました。

逆に"!(...)"の項目は、passした認証技術が1つもなく、括弧内に示された認証技術の組み合わせが失敗した割合を示しています。図-4からは、SPF単体で認証に失敗した割合"!(SPF)"が最も多く、6.5%であったことが分かります。送信ドメイン名を詐称している可能性もありますが、SPFが正しく認証できない利用例であるメール転送されて受信した割合も少なからず含まれているのではと推測しています。

次に、DMARC認証できたドメイン名のTLD(Top LevelDomain)別の割合を図-5に示します。もっとも数が多かったTLDは、com

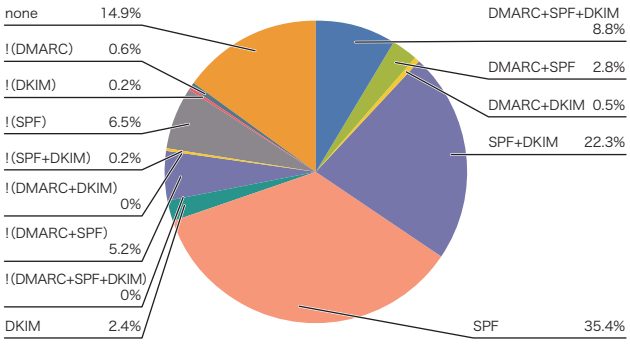

図-4 送信ドメイン認証結果の組み合わせ(2018年4月)

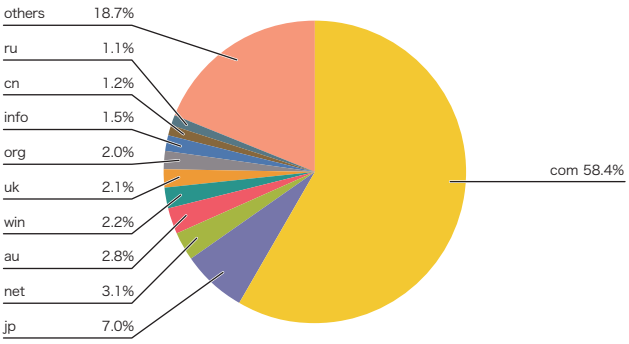

図-5 DMARC認証できたドメイン名のTLD別の割合

*5 総務省:統計データ(http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei)。

ドメイン(58.4%)でした。次がjpドメイン名(7.0%)でしたが、comドメインとの差はかなり大きい結果となりました。国の行政機関レベルで導入を働きかけている豪州[*6](au、4位、2.8%)や英国[*7](uk、6位、2.1%)も、日本での受信メールのことを考えれば、かなり高い割合であると言えます。

流量ベースでは、comが53.6%、jpが43.4%となり、これら2つのTLDで、DMARCドメイン名の大部分を占める結果となりました。

豪州と英国の行政機関へDMARC導入を働きかけていると述べましたが、米国も国土安全保障省(DHS)が連邦機関に対して、電子メールとウェブのセキュリティ強化を決定しました(BOD 18-01)[*8]。この決定では、90日以内にDMARCレコードを少なくとも"p=none"のポリシーで設定することを求めています。更に1年以内に"p=reject"と設定しなければなりません。既に報告しているとおり、"p=reject"とDMARCレコードのポリシーを設定している場合、DMARC認証が失敗したときにメールの受信を拒否される可能性が高くなります。つまり、"p=reject"と宣言するためには、SPF、DKIMの設定を含めて、正規のメールがDMARC認証で失敗しないようにメールシステムをきちんと管理していく必要があります。その意味でも米国DHSは大変重要な決定をしたと言えます。日本の政府や自治体なども検討していただくことを希望しています。

1.3.2 jpドメインの導入状況

2005年4月から2012年5月まで、WIDEプロジェクトはjpドメイン名を管理する日本レジストリサービス(JPRS)と共同研究契約を結び、jpドメイン名でのSPFなどの普及率を計測してきました[*9]。この期間は、ちょうどSPFの普及時期と重なり、その変化の度合いやその効果を類推する上で、貴重なデータとなりました。

今回、DMARC普及を進めて行くにあたり、総務省はこの調査をDMARCも含めて改めて開始することにしました[*10]。具体的な方法としては、総務省の業務委託先である(一財)日本データ通信協会がJPRSと共同研究契約を結ぶことになりました。この調査に関しては、日本データ通信協会の客員研究員の立場で筆者も参加しています。

総務省が発表した2018年1月時点での調査結果[*5](表-1)では、メールに利用するドメイン名のSPF設定割合は全体で56.9%でした。WIDEプロジェクトで調査していたSPFの普

属性	ドメイン数	MX設定数	SPF設定数	SPF設定率(%)	DMARC設定数	DMARC設定率(%)
ad	252	212	140	66.0	6	2.8
ac	3596	3367	2086	62.0	10	0.3
co	403955	380239	252961	66.5	1089	0.3
go	582	428	395	92.3	1	0.2
or	35146	33012	21043	63.7	71	0.2
ne	13044	10617	5590	52.7	99	0.9
gr	6112	5438	2884	53.0	27	0.5
ed	5230	4852	2854	58.8	21	0.4
lg	1652	1216	921	75.7	2	0.2
地域・都道府県型	13414	7530	3959	52.6	28	0.4
汎用	988365	756800	391728	51.8	5565	0.7
合計	1471349	1203711	684561	56.9	6919	0.6

表-1 jpドメインの送信ドメイン認証技術設定調査結果

＊6 DMARC、"Australian Government Agency Recommends DMARC, DKIM, and SPF"(https://dmarc.org/2016/08/australian-government-agency-recommends-dmarc-dkim-and-spf/)。
＊7 DMARC、"DMARC Required For UK Government Services By October 1st"(https://dmarc.org/2016/06/dmarc-required-for-uk-government-services-by-october-1st/)。
＊8 DHS、"Binding Operational Directive 18-01"(https://cyber.dhs.gov/bod/18-01/)。
＊9 WIDEプロジェクト、「ドメイン認証の普及率に対する測定結果」(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)。
＊10 総務省、「JPドメイン名における送信ドメイン認証技術の設定状況の調査」(http://www.soumu.go.jp./menu_news/s-news/01kiban18_01000035.html)。

及率は、MXレコードを設定したドメイン数に対する、全体でのSPFレコード設定数の割合でしたので、上記の普及率とは少し計算方法が異なります。同じ条件では、2018年1月時点で58.1%となります。WIDEプロジェクトでの2012年5月時点での普及率は43.89%でしたので、同じ条件では約14.2%増加したことになります。

jpドメイン名に対するDMARCレコードの設定調査は、今回が初めての試みとなります。IIJのメールサービスにおける受信メール比(流量比)での普及率は19.3%でしたが、実際のjpドメインでの設定割合は、残念ながら全体の平均でわずか0.6%でした。WIDEプロジェクトによる最初のSPFの調査結果が0.1%でしたので、今後の伸びに期待したいところです。また、英国や豪州、米国の政府機関での取り組みを紹介しましたが、日本政府機関での普及も期待したいところです。実際、SPFについては、政府機関が利用するgo.jpドメインで92.3%と高い普及率となっています。地方自治体でよく利用されるlg.jpドメインについても75.7%と、属性型別で2番目に高い普及率となっています。

DMARCレコードの設定は、メールサーバの出口を確認しなければならないSPFレコードの設定より更に簡単ですので、既にSPFレコードを設定できているのであれば、まず"p=none"ポリシーのDMARCレコードから設定するべきと考えています。

1.3.3 関連技術も含めた標準化動向

DMARCなどのインターネット上のいわゆる技術標準は、IETF(Internet Engineering Task Force)[*11]でRFC(Requestfor Comments)として文書で公開されます。IETFでは、議論の対象分野ごとにWG(Working Group)が作られ、WG内で技術仕様などを議論し、最終的にRFCが発行されます。今回、2018年3月に開催されたIETF 101 meetingに参加したので、最近のIETFやメール関連の状況について報告します。

IETF meetingは年3回開催されます。概ね欧州や北米、アジア地域が開催場所として選ばれます。IETF 101 meetingは欧州のロンドンで開催されました。次回のIETF 102 meetingはカナダのモントリオールで7月に開催予定となっています。参加者数はIETF 101 meetingで1,189名と報告されました。WGごとに会議室と時間帯があらかじめ設定され、複数のWG会合が同時に開催されます。通常、1つのWGは1度会合が設定されますが、参加者が多くより議論が必要と判断されるWGについては複数回の会合が催されます。また、WGによっては会合

*11 IETF(https://www.ietf.org)。

自体が開催されないこともありますので、IETF meetingに参加する場合には、あらかじめ会合のスケジュールを確認する必要があります。最近では、会場に直接参加せず、オンラインで参加する人も増えています。しかし、意見などを言いたい場合にはやはり会場に直接参加する方が良いでしょう。

IETFのdmarc WGではDMARCの仕様をRFC7489として発行しましたが、現在はARC（Authenticated Received Chain）の仕様検討を行っています。また、Informational RFCとして発行されたDMARCについても、標準化を目指すStandard Trackとするための改善の検討（主にメール再配送問題への対処など）や、DMARCレポートに含まれる情報についての検討なども行っています。

他にメールに関連するWGとしては、DKIMに対しての暗号アルゴリズムや鍵長の追加を検討するdcrup WG、JSON形式のデータを利用してIMAPやSMTPに代わる新しいアクセスプロトコルであるJMAPを検討するjmap WGなどが現在も活動中です。

IETFでの議論には原則として誰でも参加できますので、広い意見を集めることができる反面、なかなか技術仕様が固まらず、長い時間がかかってしまう、という課題もあるようです。メール関連技術に関しては、M^{3}AAWG[*12]内で検討や相互疎通テストなどが行われますので、比較的迅速にRFC化されているようです。

1.3.4 法的な整理

SPFやDKIM、DMARCを受信側で導入するためには、認証のためにメール配送上の情報やメール本文を参照する必要がありますので、原則としてメール利用者から参照することについての同意を得なければなりません。このうち、SPFとDKIMについては、送信ドメイン認証によって大量に送信される詐称メールを判断できるようになることから、認証結果のラベリングについては、一定の条件のもとで、事前に同意を得ていなくても正当業務行為として違法性が阻却できると判断されました[*13]。

一方、新しい送信ドメイン認証技術であるDMARCでは、送信側のドメイン管理者が、DMARCレコードに設定するポリシーの値で、認証が失敗したメールの処理方法を指定することができます。これにより、例えばポリシーを"p=reject"と設定すれば、多くの詐称メールの受け取りを拒否し、メール受信者に不要なメールを届ける必要もなくなります。しかしながら、これまでのSPF、DKIMなどの送信ドメイン認証技術の法的整理では、認証結果のラベリングまで整理されており、DMARCのように受信時の受け取りを拒否する処理まで整理されていませんでした。

＊12 M^{3}AAWG（https://www.m3aawg.org）。
＊13 総務省、「送信ドメイン認証技術等の導入に関する法的解釈について」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html）。

こうした背景から、迷惑メール対策推進協議会などを中心として検討を重ね、最終的に新たに受信側の処理方法を含め、DMARCを導入する上での課題について整理されました。その内容については、総務省から公開されています[*13]。この整理については、DMARCのポリシーに基づく受信側の処理方法とDMARCレポートについて述べられています。DMARCレポートには、集約レポート(aggregate report)と失敗レポート(failure report)の2種類があります。このうち、集約レポートは包括同意により個別の同意を必要とせず、受信メール側が送信ドメイン側に送信することができます。失敗レポートは、エラーメールと同様に元の送信メールの内容が含まれます。そのため、メールの通信当事者とは限らないドメイン管理者への送信は慎重に考えるべきだ、との判断がなされました。よって、包括同意によって失敗レポートを送信する場合には、元の送信されたメールの本文や件名(Subject:ヘッダの内容)を含まないこと、という条件が付きました。失敗レポートの目的の1つは、本当に送信したメールが認証失敗したのか、詐称されたメールなのかを判断することです。元の送信メールが完全な形で含まれていなくても、失敗レポートに含まれる他のヘッダ情報などから、ある程度正規のメールかどうかを判断できるはずですので、現在の制約でも十分有益な情報であると考えています。

これらの整理により、SPF、DKIM、DMARCが受信側も含めて導入が進むことを期待しています。

1.4 おわりに

迷惑メール対策の関係者が参加する「迷惑メール対策推進協議会」が、今年(2018年)で設立10年となります[*14]。その間の2014年には、迷惑メール対策に関する国際的な行政機関の会合であるLAP(London Action Plan、現在はUCEnet)の10年目の会合としてLAP 10 Tokyoが日本で開催されました。更に同じ2014年には、筆者が創設から継続して参加してきたM^{3}AAWGの10周年記念会合が米国ボストンで開催されました。

10年といえば以前は「ひと昔」でしたが、ドッグイヤーのIT業界では、区切りというよりかなりの時間が経過してしまったと言えます。にもかかわらず、迷惑メールの問題がなかなか良くなったように見えない現状には、長い間関わってきた者の1人として、少なからず責任を感じます。しかし、最悪の状況、メールが使われなくなる可能性もあったことを考えれば、それと同時に、多少の貢献ができたのでは、とも思います。実際、モバイルデバイスなどを中心に、チャット系のアプリケーションが複数利用されている状況をみれば、今後もコミュニケーションツールの利用形態は十分に変化する可能性があるとも考えています。本来、こうした新しい仕組みを考える立場でもありますので、現状のメールの課題に取り組みつつ、新しいコミュニケーションの仕組みや、そこで同じような問題が発生しないような検討を続けていきたいと考えています。

執筆者:
櫻庭 秀次(さくらば しゅうじ)
IIJ ネットワーク本部 アプリケーションサービス部 担当部長。
コミュニケーションシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織と協調した各種活動を行う。M^{3}AAWGの設立時からのメンバー。迷惑メール対策推進協議会 座長代理、幹事会 構成員、技術WG 主査。一般財団法人インターネット協会 迷惑メール対策委員会 委員長。Email Security Conference プログラム委員。一般財団法人日本データ通信協会 客員研究員。

*14 迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/anti_spam/index.html)。