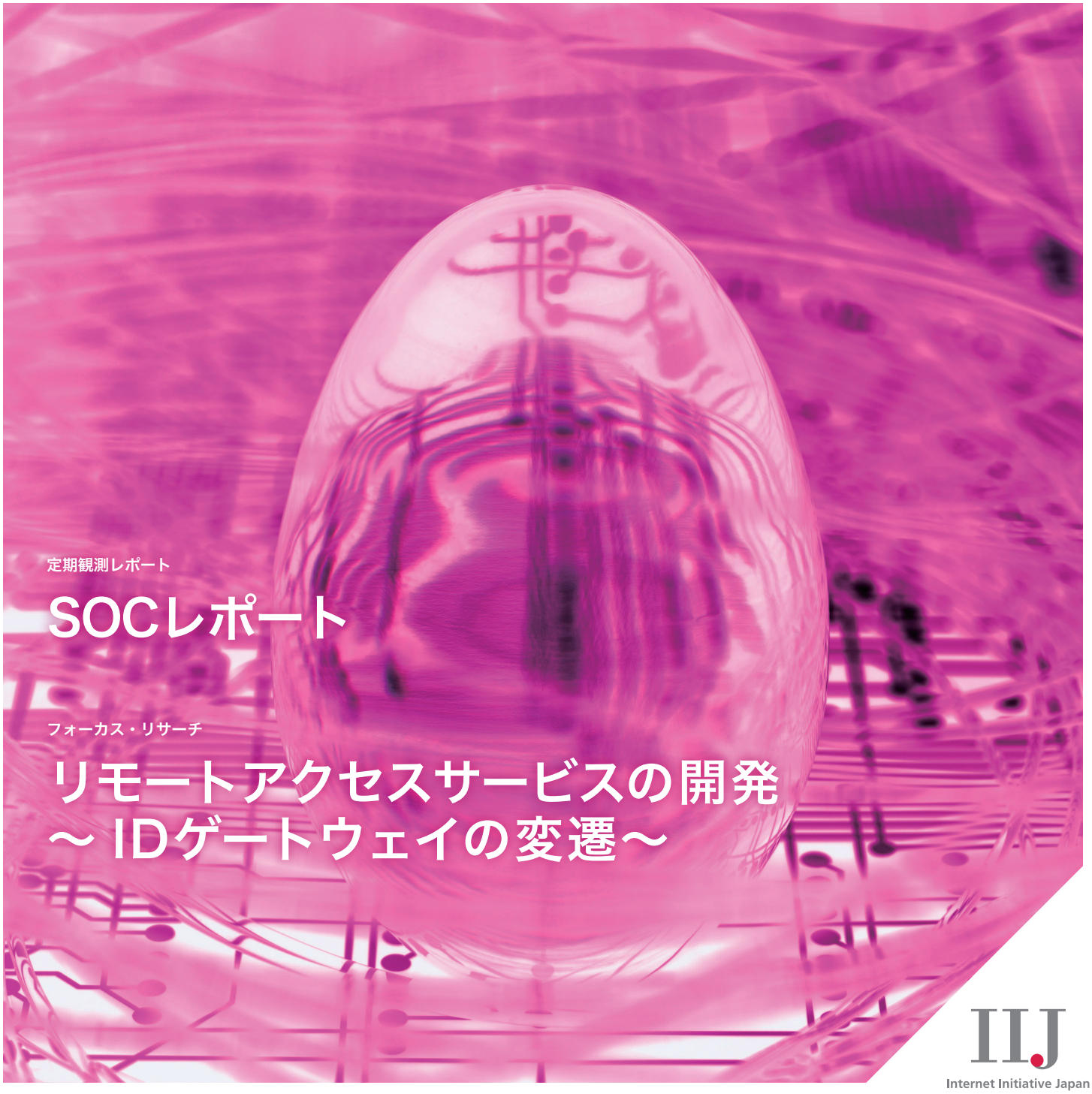
IIR

Internet
Infrastructure
Review

Mar.2025
Vol. 66



定期観測レポート

SOCレポート

フォーカス・リサーチ

リモートアクセスサービスの開発
～IDゲートウェイの変遷～

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2025 Vol.66

エグゼクティブサマリ

バルセロナで恒例の「モバイルワールドコングレス（MWC）」が開催されるなか、本稿を執筆しています。ご存じの方も多いかと思いますが、MWCは移動通信事業者や端末・機器を製造するメーカなど、移動通信に関連する企業による業界団体「GSM Association」が主催する移動通信業界における最大のイベントです。

本年のMWCのテーマは「Converge. Connect. Create.」ですが、過去5年のテーマを振り返ると「Velocity」、「Connected Impact」、「Connectivity Unleashed」、「Connected Impact」、「Limitless Intelligent Connectivity」でした。移動通信業界のイベントということで、継続して「Connectivity」がフォーカスされているものの、他のIT関連イベントと同様に、AIが注目を集め、「Beyond Connectivity」というキーワードも使われています。

世界的にも5Gのマネタイズに苦労していると言われ、通信事業以外のビジネスをいかに拡大するかという議論がある一方、そのようなビジネスを可能にするためのインフラはどうあるべきか、どのような技術開発が必要か、といったことも活発に議論されています。伝統的な「Connectivity」だけに囚われない新しいサービスと、それを可能にする新しいインフラを創っていくことは、通信事業者である私たちの重要なミッションであります。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されます。

1章の定期観測レポートは、毎年恒例の「SOCレポート」です。前年に発生した主要なセキュリティトピックのうち、IIJのSOCが注目したものを振り返ると共に、今年はDDoS攻撃について深堀りしています。2024年も1年を通じて多くのDDoS攻撃が観測されましたが、日本では24年末から25年の年初にかけてDDoS攻撃が継続的に発生し、社会生活にも影響を及ぼした事案が報道されました。そのようなDDoS攻撃の手法や傾向について述べたうえで、多くのDDoS攻撃で利用されている「Mirai」とその亜種の解析支援ツール「mirai-toushi」を解説しています。

2章の「フォーカス・リサーチ」は、IIJが26年間提供した「IDゲートウェイサービス」の裏側を紹介します。現在では、移動通信ネットワークやクラウドサービスの進化により、いつでも・どこからでも、必要な情報やそれを処理するコンピューティングリソースにアクセスできます。IDゲートウェイサービスが開始された1998年は、まだダイアルアップによるインターネット接続が主流であり、情報もコンピューティングリソースも企業のネットワークのなかにありました。サービス開始以来、IDゲートウェイサービスは技術の進化や社会の変化に応じて改良が加えられてきましたが、それを支えるIIJの内製ソフトウェアの歴史を振り返ってみました。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながら、日々改善し発展させていく努力を続けています。今後も、企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けてまいります。

島上 純一（しまがみ じゅんいち）
IIJ 取締役 専務執行役員 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任し、2023年5月に退任。2021年6月より同協会の副会長に就任。

SOCレポート

1.1 はじめに

IIJではセキュリティブランド「wizSafe」を2016年に立ち上げ、お客様が安全にインターネットを利用できる社会の実現に向けた活動を続けています。その活動の一つに「wizSafe Security Signal」[*1]による定期的なセキュリティに関する情報発信があります。掲載している情報はIIJサービスのセキュリティログを集約している情報分析基盤を活用したもので、日々収集している脅威情報と組み合わせた様々な角度からセキュリティ分析を行っています。

本稿では、第1.2節にて2024年に発生した主要なセキュリティトピックについてカレンダー形式で振り返り、社会的な影響から改めて注目を集めたDDoS攻撃に関連する観測情報を第1.3節にて紹介します。観測情報にはIIJサービスで検知したDDoS攻撃の発生状況をはじめ、昨今のDDoS攻撃において重要な要素となっているIoTマルウェアの感染活動を取り上げます。第1.4節ではIoTマルウェアの解析を効率化するために開発した解析支援ツール「mirai-toushi」を紹介します。

1.2 2024年セキュリティサマリ

2024年に話題となった主要なセキュリティに関する出来事の中から、SOCが注目したものを表-1と表-2にまとめます。

＊1　wizSafe Security Signal（https://wizsafe.iij.ad.jp/）。

表-1 セキュリティトピックカレンダー（1月～5月）

月	概要
1月	**Ivanti社製品の脆弱性** Ivanti社は、Ivanti Connect Secure（旧: Pulse Connect Secure）及びIvanti Policy Secureゲートウェイに複数のゼロデイ脆弱性（CVE-2023-46805、CVE-2024-21887）が存在することを公表した。これらの脆弱性を組み合わせることで認証不要の任意のコマンド実行が可能となる。脆弱性の公開時点では修正バージョンがリリースされておらず、既に広く悪用されている状態であった。修正バージョンのリリースの際には権限昇格の脆弱性（CVE-2024-21888）とSSRFの脆弱性（CVE-2024-21893）も併せて修正されており、CVE-2024-21893はリリース以前から悪用されていたことが報告されている。
1月	**Citrix社製品の脆弱性** Citrix社は、NetScaler ADC及びNetScaler Gatewayに存在する脆弱性（CVE-2023-6548、CVE-2023-6549）を公表した。CVE-2023-6548はリモートコード実行、CVE-2023-6549はサービス拒否（DoS）につながる恐れがあり、いずれも情報公開時には既に悪用されていたことが確認されている。
2月	**SonicWall社製品の脆弱性** SonicWall社は、同社が提供するSonicOSのSSL-VPN機能に不適切な認証の脆弱性（CVE-2024-22394）が存在することを公表した。この脆弱性により認証をバイパスされる恐れがある。
2月	**Fortinet社製品の脆弱性** Fortinet社は、同社が提供するFortiOS及びFortiProxyに境界外書き込みの脆弱性（CVE-2024-21762）が存在することを公表した。この脆弱性により、任意のコードまたはコマンドを実行される恐れがある。また、当該脆弱性は既に悪用されていたことが確認されている。
2月	**ランサムウェアLockBitに対する国際的な取り組み** Europol（欧州刑事警察機構）は、ランサムウェア「LockBit」を用いるサイバー犯罪グループに対する共同捜査を実施し、所属メンバー2名の検挙と攻撃インフラを掌握したことを公表した。この共同捜査は日本を含む10カ国の法執行機関が参加しており「Operation Cronos」と名付けられている。その後、新たなLockBitのリークサイトが立ち上げられ攻撃活動は再開し、10月にはOperation Cronosの一環としてLockBitの開発者を含む4名の追加逮捕と攻撃インフラの一部サーバの押収を公表している。
2月	**脅威アクター関連情報のリーク** 中国のセキュリティ企業の内部資料と思われるデータがGitHubにアップロードされたことが確認された。米国のセキュリティ企業によると、中国とのつながりが指摘されている脅威アクターが用いるツールの開発サポートを行っていたことを示す内容であったとのこと。
3月	**経済団体におけるサポート詐欺被害** 経済団体は、ネットバンキングの不正送金によって合計1,000万円の金銭的被害を受けたことを公表した。偽の警告画面をブラウザ上に表示するサポート詐欺の手口により、業務用のパソコンに遠隔操作ソフトウェアをインストールしたことに起因している。
3月	**ソフトウェア開発会社における個人情報漏えい事件** ソフトウェア開発会社は自社提供サービスにおいてストレージサーバのアクセス制限の誤設定により、顧客の個人情報が漏えいしていたことを公表した。5月の調査報告によると個人データの漏えいした人数は158,929人であり、報告時点では個人データの不正利用などの二次被害は確認されていない。
3月	**XZ-Utilsの脆弱性** The Tukaani Projectはファイル可逆圧縮ツールであるXZ-Utilsに悪意のあるコードが挿入された問題（CVE-2024-3094）を公開した。特定の条件下において、外部からSSHポートを経由して接続される恐れがある。XZ-Utilsは複数のLinuxディストリビューションで利用されており、影響を受けるシステムは多岐にわたった。
4月	**レンズメーカにおけるサイバー攻撃被害** レンズメーカは、同社のシステムにおいて障害が発生し、生産工場内のシステムや受注システムが停止していることを公表した。システム障害の原因は第三者によるサイバー攻撃であり、4月23日時点で概ね復旧したと報告している。この事象により取引先の複数の販売店にて一部レンズの取り扱いが停止するなど、直接攻撃を受けた企業以外にも影響が見られた。
4月	**Palo Alto Networks社製品の脆弱性** Palo Alto Networks社は、PAN-OS GlobalProtectにOSコマンドインジェクションの脆弱性（CVE-2024-3400）が存在し、脆弱性を悪用する攻撃が既に確認されていることを公表した。
5月	**鉄道会社におけるDDoS攻撃被害** 鉄道会社の提供するインターネットサービス（決済システムなど）において接続がしづらい状態となった。このシステム障害はIC乗車券に関連するシステムへのサイバー攻撃が原因であり、DDoS攻撃の疑いがあると報道されている。
5月	**Check Point Software Technologies社製品の脆弱性** Check Point Software Technologies社は、同社の提供するセキュリティゲートウェイ製品に情報漏えいの脆弱性（CVE-2024-24919）があり、パスワード認証による不正なログイン試行攻撃が確認されていることを公表した。
5月	**国内の暗号資産取引所におけるビットコイン不正流出** 国内の暗号資産取引所は当時の価格レートで約482億円相当のビットコインが不正流出したことを公表した。同年9月には関東財務局より資金決済に関する法律第63条の16に基づき行政処分（業務改善命令）を受け、原因究明と顧客対応などについて報告の対応が求められた。12月には別の国内暗号資産取引所に顧客資産を移管しサービス事業を廃止することを発表した。その後、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）と警察庁の連名で当該事案は北朝鮮を背景とする攻撃グループのTraderTraitorによる犯行であったとの情報が公開された。公開された文書では、被害を受けた暗号資産取引所が利用していた暗号資産ウォレットソフトウェアの開発企業の従業員に対して、攻撃者がリクルーターを装い接触するなどのソーシャルエンジニアリングの手口などが言及されている。
5月	**システム開発会社におけるランサムウェア被害** システム開発会社は、同社のサーバやPCにおいてファイルが暗号化されるランサムウェアの被害を受けたことを公表した。その後の調査で侵入経路がVPNであること、窃取された情報が攻撃グループのリークサイト上で一時的に公開され、その情報に取引先の顧客に関する個人情報が含まれていたことを報告している。本事案により同年9月にISO27001認証及びISO27017認証、12月にプライバシーマーク付与が一時停止となった。また、当該システム開発会社に業務を委託していた多数の企業や自治体から個人情報の漏えいに関する報告が出るなど本事案による被害は多岐に渡った。

表-2 セキュリティトピックカレンダー(6月〜12月)

月	概要
6月	**エンターテインメント企業におけるランサムウェア被害** 出版やWebサービス、教育事業などを手掛けるエンターテインメント企業は、ランサムウェア攻撃により出版やWebサービス事業、MD事業など多岐にわたる機能停止が発生していることを明らかにした。攻撃による影響を受けた事業活動は順次復旧作業が行われ、同年8月から9月にかけて平常時と同等の水準に出荷数などは回復、サービスについても全面的な復旧となったことが報告された。また、攻撃グループは当該企業から窃取した情報を流出させたと複数回に渡り主張している。調査の結果、最終的に254,241人の個人情報及び社内外の企業情報の流出が確認された。
7月	**セキュリティ製品の不具合による大規模障害発生** 米国セキュリティ企業が提供するエンドポイントセキュリティ製品において、Windows向けアップデートで配信された一部のファイルに不具合があり、アップデートされたホストがクラッシュする障害が世界各地で相次いだ。この事象により航空便の欠航や遅延、小売店舗のPOSレジが使用不可になるなど幅広い業種が影響を受けた。
7月	**DDoS攻撃代行サービスに対する国際的な取り組み** 英国国家犯罪対策庁(NCA)は、Police Service of Northern Ireland(PSNI)及びFBIによる捜査が行われDDoS攻撃代行サービス「digitalstress」のプラットフォームを押収し、管理者と疑われる者は逮捕したことを公表した。この作戦はDDoS代行サービスを閉鎖するための共同作戦「Operation Power Off」の一環として実行された。
8月	**DDoS攻撃代行サービス利用者の逮捕** 複数のメディアは、DDoS攻撃の代行サービスを利用して、国内のWebサイトに攻撃を行っていた男が警察庁により逮捕された旨を報じた。DDoS代行サービスに対しては「Operation PowerOFF」と呼称される国際的な共同捜査が遂行されている。また、DDoS代行サービスの利用による別件の検挙事例が11月と12月にも相次いで報道されている。
9月	**SonicWall社製品の脆弱性** SonicWall社は8月に公開したSonicOSの不適切なアクセス制御の脆弱性(CVE-2024-40766)について、管理アクセスインタフェースのみでなくSSL-VPN機能も影響を受けるとしてセキュリティアドバイザリの内容を更新した。この脆弱性により、認証不要でリモートから攻撃が可能となる。同社からは製品のアップデートの他、ローカルユーザのパスワード変更や多要素認証の有効化、SSL-VPNログインのログ取得、アカウントロック機能などが推奨されている。
9月	**物流サービス会社におけるランサムウェア被害** 物流サービス会社は、複数のサーバがランサムウェア攻撃を受けたことを公表した。業務に関連した複数のシステムが停止したことで、取引先の入出庫処理に停止または遅延が発生した。被害公表の当初、攻撃による個人情報の漏えいの可能性に言及していたが、同年10月にリークサイトなどへの情報公開は行われていないことから情報漏えいの事実は確認されていないと報告された。また、サプライチェーンで同社のサービスを利用していた複数の企業からも攻撃による影響について報告が出されている。
10月	**保育施設運営会社におけるランサムウェア被害** 保育施設運営会社は、同社のサーバがランサムウェア攻撃を受けたことを公表した。公表時点では個人情報が漏えいした可能性について言及されていたが、同年11月の追加報告によると外部専門家による調査により、サーバ内の個人情報を閲覧された可能性はあるが、データが持ち出された形跡は確認されなかったとしている。また、同社に施設の運営を委託している複数の自治体からもサイバー攻撃被害について報告されている。
10月	**損害保険鑑定会社におけるランサムウェア被害** 損害保険鑑定会社は、同社のサーバがランサムウェアに感染したことを公表した。調査により、UTM機器へのブルートフォース攻撃後、サーバにRDP接続することで侵入された可能性が報告されている。個人情報の漏えいにつながる情報は確認されていないが、ローカルフォルダへの不正なアクセスや事象のあった時間帯についてログが削除されていることから、漏えいの可能性について否定できないとしている。また、サプライチェーンで同社のサービスを利用していた複数の企業からも攻撃による影響について報告が出されている。
10月	**Fortinet社製品の脆弱性** Fortinet社は、同社が提供するセキュリティ管理プラットフォーム「FortiManager」のfgfmdデーモンにおいて認証の欠如の脆弱性(CVE-2024-47575)が存在することを公表した。この脆弱性により、リモートで任意のコードまたはコマンドを実行される恐れがある。また、当該脆弱性は公開時点で既に悪用されていたことが確認されている。
11月	**Palo Alto Networks社製品の脆弱性** Palo Alto Networks社は、PAN-OSのWeb管理インタフェースにおいて、認証をバイパスできる脆弱性(CVE-2024-0012)と権限昇格が可能となる脆弱性(CVE-2024-9474)が存在することを公表した。また、当該脆弱性は公開時点で既に悪用されており、製品上でのコマンド実行やWebShellの配置などが行われていたことが確認されている。
12月	**国内におけるDDoS攻撃被害の多発** 国内の航空会社や金融機関を中心に大量のデータを送付されるDDoS攻撃に起因したとされるサービス障害が相次いで発生した。これにより、当該企業の運用するWebサービスや航空機の運航に影響が生じた。

1.3 DDoS攻撃トピックス

1.3.1 DDoS攻撃観測情報

本節ではIIJサービスにて検知されたDDoS攻撃について紹介します。表-3は2024年に検出した攻撃を月ごとに要約したものです。

2024年に観測された最も規模の大きな攻撃は174.80Gbpsの通信が発生したもので、攻撃手法はDNSを利用したUDP Amplificationが用いられていました。また、最も長く継続した攻撃はおよそ3時間24分にわたるもので、TCP SYN Floodが利用されていることを確認しています。その他に観測されているDDoS攻撃についても、攻撃規模に関わらずUDP AmplificationやTCP/UDP Floodといった同様の攻撃手法が用いられており、以前から観測されている手法から大きな変化はありませんでした。

2024年12月に観測した攻撃のうちUDP Floodを行っていた送信元IPアドレスについて外部情報サイトを用いて調査したところ、情報を取得できたIPアドレスの半数以上がTP-Link社製のルータやHikvision社製のIPカメラなどIoT機器のものでした。これらの機器は初期パスワードが固定されたものです。初期パスワードが変更されていないため、外部からのログインが可能な状態であったものと思われます。

IoT機器の利用が一般化する中、セキュリティ対策などの運用面は意識が希薄になりがちです。そのため、脆弱な状態のまま稼動している端末が世界中に多く存在し、それらを対象とする攻撃も活発に行われています。攻撃が成功した場合、IoTマルウェアに感染し本項で紹介したようなDDoS攻撃に加担してしまう恐れがあります。初期パスワードを予測されにくいパスワードに変更することやファームウェアを最新のものに更新する、またはサポート終了している場合は端末の利用を停止するなどの対策が重要です。

1.3.2 ハニーポットで観測したIoT機器を狙った攻撃通信の傾向

IIJではハニーポット[*2]へのIoT機器を対象とした攻撃についても情報分析基盤に連携し分析・活用しています。IoT機器が外部からの攻撃によってIoTマルウェアに感染した場合、DDoS攻撃などを行うボットネットワークの構成要素として悪用される恐れがあります。本項では、IIJのハニーポットで観測したIoTマルウェアの感染活動について紹介します。

表-3 DDoS攻撃検出状況（2024年）

	最も規模の大きな攻撃に関する観測情報				最も長く継続した攻撃に関する観測情報	
月	検出件数（1日あたりの平均）	パケット数（万pps）	帯域（Gbps）	主な攻撃手法	継続時間	主な攻撃手法
1	7.58	533	2.47	TCP SYN/ACKリフレクション攻撃	13分	TCP SYN Flood
2	9.79	690	71.11	DNSプロトコルを用いたUDP Amplification	25分	TCP ACK Flood
3	7.61	6	0.61	HTTP Flood	1時間41分	HTTP Flood
4	7.97	526	54.90	複数のプロトコル（WSD、SADP、CoAPなど）を組み合わせたUDP Amplification	39分	複数のプロトコル（WSD、SADP、CoAPなど）を組み合わせたUDP Amplification
5	9.13	70	8.15	HTTP Flood	16分	HTTP Flood
6	13	1228	110.88	DNSプロトコルを用いたUDP Amplification	1時間10分	TCP ACK Flood
7	10.87	1050	90.64	UDP Flood	3時間24分	TCP SYN Flood
8	12.23	426	44.34	DNSプロトコルを用いたUDP Amplification	12分	DNSプロトコルを用いたUDP Amplification
9	8.4	262	9.74	NTPプロトコルを用いたUDP Amplification	2時間3分	NTPプロトコルを用いたUDP Amplification
10	7.77	477	49.63	DNSプロトコルを用いたUDP Amplification	12分	DNSプロトコルを用いたUDP Amplification
11	7.23	1680	174.80	DNSプロトコルを用いたUDP Amplification	1時間14分	DNSプロトコルを用いたUDP Amplification
12	7.06	332	12.12	UDP Flood	2時間3分	UDP Flood

＊2　IoT機器に対応したハニーポットについては、本レポートのVol.36「フォーカス・リサーチ（1）」（https://www.iij.ad.jp/dev/report/iir/036/02.html）にて詳細を説明しています。

IoT機器には、インターネット上からTELNETを用いてログイン可能な製品が多数存在します。このTELNETに必要なユーザとパスワードが、製品の初期設定のまま運用されているケースがあり、これがIoTマルウェア感染の入口の一つとなっています。「Mirai[*3]」に代表されるボットネットワークを構成するIoTマルウェアは、その感染範囲を拡大するためにランダムなグローバルIPアドレスに対してTELNETサービスをスキャンする挙動が知られています。

ハニーポットでは、広範なグローバルIPアドレスへのスキャン活動や攻撃を観測することが可能であり、送信元となる端末数の増加などと組み合わせて特定のIoTマルウェアの感染拡大などを捕捉することも期待されます。ただし、MiraiなどのIoTマルウェアはそのソースコードが公開されているものがあり、それらを改変した様々な亜種が存在しています。そのため、もともとのソースコードで確認されていた通信の特徴や攻撃通信の内容から変化する場合があることに注意が必要です。

2024年にハニーポットで観測したTELNET（23/TCP、2323/TCP）宛の攻撃通信について、Miraiの特徴[*4]を持った送信元とMiraiの特徴を持たない送信元に分けて送信元IP数の変化と攻撃通信の内容を分析した結果を以降に示します。

Miraiの特徴を持った送信元IPアドレス数（観測期間の最大値で正規化）の推移について攻撃通信の内容に基づいて分類した結果を図-1に示します。調査の結果、10月に「gayfgt」を16進数エスケープした文字列（\x67\x61\x79\x66\x67\x74）をechoコマンドで実行する内容を含む送信元（「グループA」と分類）、及び「/bin/busybox NUG」のコマンドを攻撃通信に含む送信元（「グループB」と分類）が顕著に増加していました。また、「グループA」については12月に再び送信元の増加が確認されました。

「グループA」と分類した攻撃通信で感染するマルウェアを調査したところ、その大半においてMirai亜種である「RapperBot」の特徴を確認しました。具体的には、これまでのRapperBotと設定情報の暗号化手法（1バイトXOR）、暗号鍵のパターン（暗号化データの末尾1バイトである）、及び設定情報に含まれるYouTubeのURLアドレスが等しいことを確認しています。なお、「グループA」の特徴である「gayfgt」の出力文字列はBASHLITE（別名Gafgyt）と呼ばれるIoTマルウェアの特徴として知られていますが、調査した検体に関しては、BASHLITEではないことを確認しています。

「グループB」と分類した攻撃通信で感染するマルウェアを調査したところ、その大半において2024年5月に観測されたMirai亜種「FICORA」の特徴の一部（設定情報の8バイトXORによる暗号化及び暗号鍵が等しいこと）を確認しました。このことから、「グループB」はFICORAもしくは類似のMirai亜種である可能性が高いです。

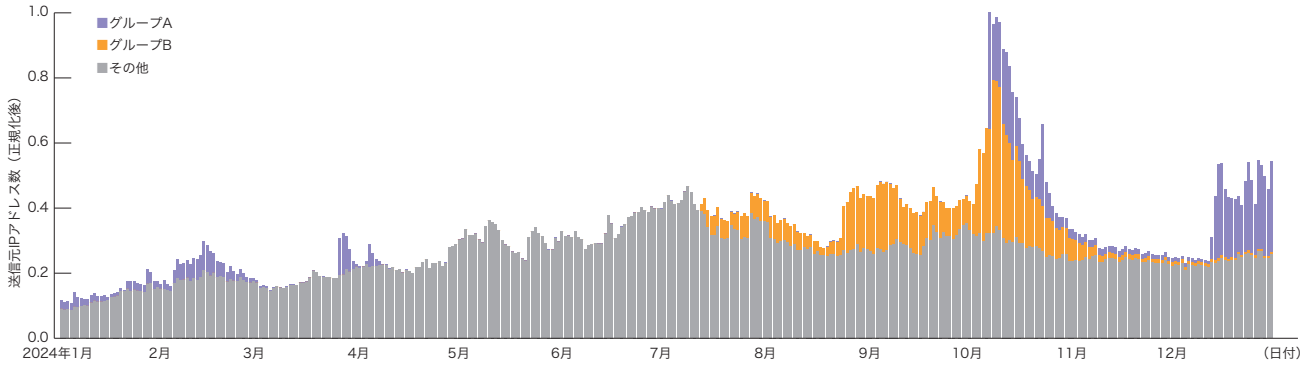


図-1 ハニーポットで観測した攻撃通信の送信元IPアドレス数（正規化後）の分類別推移（Miraiの特徴を持つ送信元）

＊3　Miraiについては、本レポートのVol.33「フォーカス・リサーチ（1）」（https://www.iij.ad.jp/dev/report/iir/033/01_04.html）にて詳細を説明しています。
＊4　TCPヘッダのシーケンス番号とIPアドレスの値が同じで、送信元ポートが1024より大きいものを指します。ただし、この特徴を持たないMirai亜種も存在しています。

続いて、Miraiの特徴を持たない送信元IPアドレス数（観測期間の最大値で正規化）の推移について攻撃通信の内容に基づいて分類した結果を図-2に示します。調査の結果、1月からは多くの送信元が「/bin/busybox hostname PBOC」のコマンドを含む攻撃通信を行っていました（「グループC」と分類）が、9月にかけて徐々に減少し、その後「/bin/busybox hostname whomp」の実行を含む攻撃通信の送信元（「グループD」と分類）が増加していたことを確認しました。

「グループC」と分類した攻撃通信で感染するマルウェアを調査した結果、その大半においてMirai亜種である「InfectedSlurs」の特徴を確認しました。具体的には、これまでのInfectedSlursと設定情報の暗号化手法（RC4とXORの組み合わせ）、暗号鍵、及びマルウェアに含まれる文字列が等しいことを確認しています。

「グループD」と分類した攻撃通信で感染するマルウェアを調査した結果、その大半において2024年4月に観測されたMirai亜種「CatDDoS」の特徴の一部（設定情報のChaCha20による暗号化、暗号鍵、及びnonceが等しいこと）を確認しました。このことから、「グループD」はCatDDoSもしくは類似のMirai亜種である可能性が高いです。

また、「グループC」と分類した攻撃通信は、国内を送信元とするものも観測しています。日本国内を送信元とするMiraiの特徴を持たない送信元IPアドレス数（観測期間の最大値で正規化）の推移を「グループC」とそれ以外に分類して示したものを図-3に示します。

「グループC」と分類した送信元IPアドレス数は昨年末からの増加した状態が2月の上旬頃まで継続し、一度減少した後に6月から7月中旬にかけて再び一時的に増加する傾向にありました。前述のとおり、「グループC」と分類した攻撃通信で感染するマルウェアの大半がInfectedSlursであり、当該期間において国内でのInfectedSlursの感染端末が増加した可能性があります。InfectedSlursについては、2023年末にIIJ-

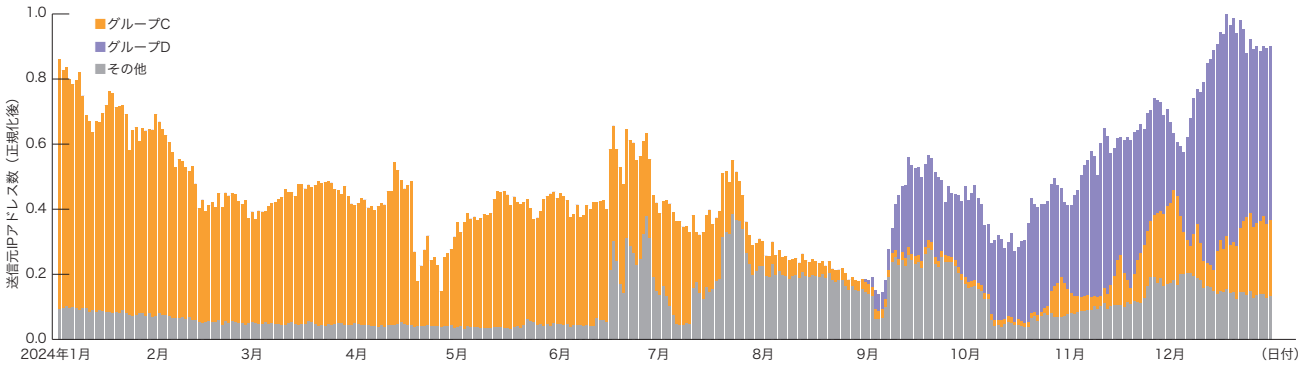


図-2 ハニーポットで観測した攻撃通信の送信元IPアドレス数（正規化後）の分類別推移（Miraiの特徴を持たない送信元）

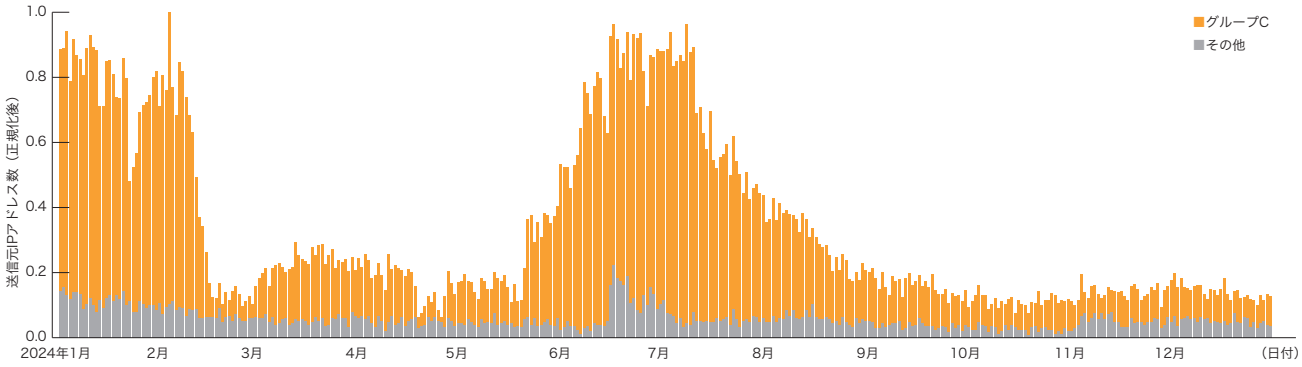


図-3 ハニーポットで観測した日本国内からの攻撃通信の送信元IPアドレス数（正規化後）の分類別推移（Miraiの特徴を持たない送信元）

SECT[*5]からも報告があるように、複数のIoT機器のゼロデイ脆弱性を悪用することや、主に日本国内で利用されている製品も感染対象とすることが確認されているため、国内の製品を利用している場合でも注意が必要です。

1.4 IoTマルウェア解析支援ツール「mirai-toushi」

IoTボットネットでは、特に2016年にソースコードが流出したMiraiとその亜種が現在でもよく使われており、日々多数のマルウェアを観測しています。攻撃者はオリジナルのソースコードをそのまま攻撃に使っているわけではなく、設定情報を編集した上でソースコードをクロスコンパイルし、攻撃に使うマルウェアを作成します。このため、ソースコードが流出しているMiraiのマルウェア解析では、オリジナルのソースコードからの変更点がある設定情報を抽出し、そのマルウェアの特徴を把握することが重要です。

マルウェアごとに手動で設定情報の抽出を行うと時間が膨大にかかってしまうため、ツールで抽出を自動化する必要があります。既存の解析ツールでもMiraiの設定情報を抽出するものは存在しますが、対応アーキテクチャ数が少ないことや、設定情報が一部しか抽出できないなどの課題がありました。このため、IIJのSOCでは独自にMiraiの設定情報抽出ツール「mirai-toushi」を開発しました。以降では、はじめにMiraiの設定情報を説明し、mirai-toushiの実装について説明します。

1.4.1 Miraiの設定情報

多くのマルウェアでは設定情報は暗号化されていることが多く、Miraiの設定情報も暗号化されています。オリジナルのMiraiでは、暗号化されている設定情報はパスワードリストとテーブルの2種類存在します（図-4）。

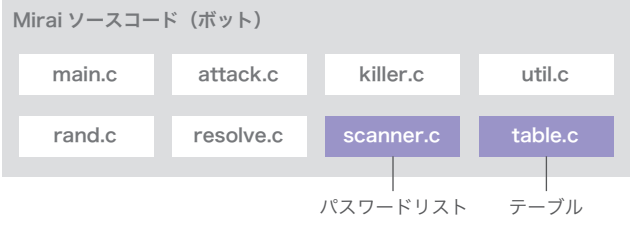


図-4 IoTマルウェアMiraiの設定情報

■ パスワードリスト

MiraiではTELNETスキャンに用いるパスワードリストがXORで暗号化されて格納されています。パスワードリストを登録する処理はソースコードのscanner.cに記述されており、scanner_init()内でadd_auth_entry()を呼び出してパスワードリストを登録します。add_auth_entry()の引数にはユーザ名・パスワード・重みが渡されます（表-4）。ユーザ名とパスワードは4バイトのXORキーで暗号化されますが、各バイトに対してXORキーを4分割した1バイトで4回XORするので、実質的に1バイトのXORキーでXORされることと同じです。例えば、XORキーが0xDEADBEEFの場合、結果として0x22でXORされることになります（byte ⊕ 0xDE ⊕ 0xAD ⊕ 0xBE ⊕ 0xEF = byte ⊕ 0x22）。重みは、パスワードリストのランダム選択の重み付き確率に用いられる値で、この値は暗号化されません。

■ テーブル

Miraiでは様々な設定情報（以下、テーブル）がXORで暗号化されて格納されています。オリジナルのMiraiのテーブルに含まれる設定情報は、C2サーバのドメインとポート番号・Scan Receiverのドメインとポート番号・標準出力に出力される文字列・敵対マルウェアのプロセスをキルするためのシグネチャ・TELNETスキャンのログイン成功後に実行するコマンド・DoS攻撃に使われるパラメータがあります。テーブルを登録する処理はソースコードのtable.cに記述されており、table_init()内でadd_entry()を呼び出してテーブルを登録します。add_entry()の引数にはID・データ・データの長さが渡さ

表-4 add_auth_entry()の引数

変数名	型	暗号化手法	説明
enc_user	char*	1バイトXOR	ユーザ名
enc_pass	char*	1バイトXOR	パスワード
weight	uint16_t	-	重み

＊5　Mirai亜種InfectedSlursの活動状況（https://sect.iij.ad.jp/blog/2023/12/mirai-infectedslurs/）。

れます(表-5)。IDはテーブルの情報を呼び出す際に使用される値です。データは4バイトのXORキーで暗号化されますが、パスワードリストと同じ理由で、実質的に1バイトでXORされることと同じです。ただし、XORキーが定義される箇所が異なるので、XORキーがパスワードリストのものと異なることがあります。

1.4.2 mirai-toushiの実装

mirai-toushiは、Ghidra[*6]のデコンパイラと中間表現のP-Codeを活用して、PythonのGhidra Scriptで実装しています(図-5)。Ghidraは、アメリカ国家安全保障局(NSA)が公開しているオープンソースのリバースエンジニアリングツールで、JavaやPythonを用いたGhidra Scriptによって解析を自動化できます。Ghidraでは対象バイナリをアセンブリに変換し、アセンブリからP-Codeに変換します。P-Codeの内容をもとにデコンパイルし、C言語のコードを生成します。P-Codeとデコンパイルされ たC言語のコードは、アーキテクチャに依存した表現ではないため、これらを活用することでクロスアーキテクチャに対応したツールを開発できます。これによってmirai-toushiでは8種類のアーキテクチャ(ARM・MC68000・MIPS・PowerPC・SPARC・SuperH4・x86・x86_64)に対応しています。以降でパスワードリストとテーブルの抽出についての実装をそれぞれ説明します。

■ パスワードリストの抽出

scanner.cに記述されるパスワードリストの抽出には、XORキーを特定する「key extractor(scanner)」とパスワードリストを復号する「decoder(scanner)」を用います。

はじめに、key extractor(scanner)で、パスワードリストの暗号化に使用されるXORキーを特定します。ソースコード上では4バイトのXORキーを4分割して4回XORしていますが、コンパイラの最適化によって、1回のXORに集約されます。このため、各関数のデコンパイル結果を取得し、データの各バイトに対して再帰的に1バイトのXORを行っている命令を特定します。この1バイトをパスワードリストの暗号化に使用されるXORキーと判定します。

次に、decoder(scanner)で、パスワードリストを復号します。パスワードリストはadd_auth_entry()で登録されるため、デコンパイル結果からadd_auth_entry()が呼び出される箇所を特定します。この際、関数の引数の数や型が正しく解釈されずに、誤ったデコンパイル結果が出力されることがあります。これに対処するため、Ghidra ScriptのupdateFunction()を用いて、関数の引数を正しく定義した上でデコンパイル結果を取得します。第一引数のユーザ名と第二引数のパスワードは特定

表-5 add_entry()の引数

変数名	型	暗号化手法	説明
id	uint8_t	-	ID
buf	char*	1バイトXOR	データ
buf_len	int	-	データの長さ

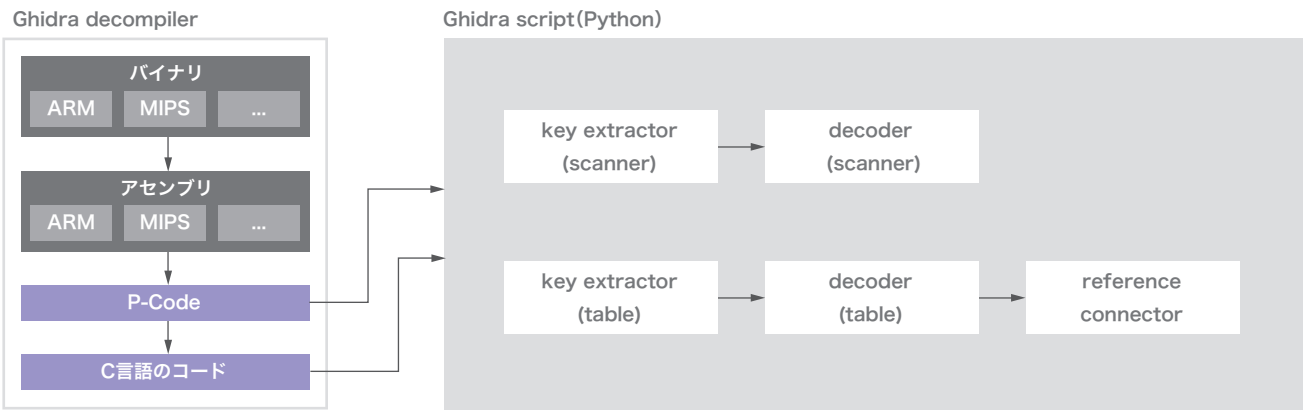


図-5 mirai-toushiの全体像

*6 Ghidra(https://ghidra-sre.org/)。

したXORキーで復号し、第三引数の重みは暗号化されないため、そのまま数値に変換します。抽出したパスワードリストはJSON形式で出力されます(図-6)。

■ テーブルの抽出

table.cに記述されるテーブルの抽出には、XORキーを特定する「key extractor(table)」、テーブルを復号する「decoder(table)」、及びテーブルの呼び出し元を特定する「reference connector」を用います。

はじめに、key extractor(table)で、テーブルの暗号化に使用されるXORキーを特定します。ここでは各関数のP-Codeを取得し、XORに相当する命令であるINT_XOR命令を取得します。対象の関数内でXORを4回行うため、この処理が含まれる関数を特定し、XORを行った4バイトを取得します。この4バイトをテーブルの暗号化に使用されるXORキーと判定します。

次に、decoder(table)で、テーブルを復号し、後続のreference connectorで使用するIDを算出します。テーブルはadd_entry()で登録されますが、コンパイラの最適化によってadd_entry()はインライン展開されます。このため、add_entry()内で呼び出されるutil_memcpy()の内容からテーブルを取得します。この際、Ghidra ScriptのupdateFunction()を用いて、関数の引数を正しく定義した上でデコンパイル結果を取得し、第二引数のテーブルのデータを特定したXORキーで復号します。2バイトのデータは、ポート番号である可能性があるので、数値として復号します。これに加えて、各データのIDを算出します。テーブルには各データが配列として格納され、IDがインデックスの役割を果たします。このため、各データのアドレスをテーブルの先頭アドレスで引いて、その値をデータのサイズで割るとIDが算出できます。データのサイズはアーキテクチャによって異なり、MC68000は6バイト、それ以外の32ビットアーキテクチャは8バイト、64ビットアーキテクチャは16バイトとなります。

最後に、reference connectorで、テーブルが呼び出される関数とアドレスを特定します。テーブルが呼び出される際は、table_retrieve_val()が呼び出されるため(例:table_retrieve_val(TABLE_CNC_DOMAIN, NULL))、各関数のデコンパイル結果を取得して、この関数が呼び出される箇所を特定します。第一引数にIDの値が入るため、decoder(table)で算出した情報と突合することで、テーブルがどの関数とアドレスで呼び出されるのか特定できます。抽出したテーブルはJSON形式で出力され、refsの値にreference connectorの結果が記載されます(図-7)。

mirai-toushiはIIJのGitHubリポジトリに公開しており[*7]、ツールをサンプルの検体に適用したときのより詳細な出力例とJSON Schemaの情報を確認できます。Ghidraがインストールされている環境であれば追加設定・ライブラリなしでツールを実行することができ、抽出した設定情報は様々な用途に活用できます。


```
{
  "scanner_init_func": {
    "auth_tables": [
      {
        "user": "root",
        "pass": "admin",
        "weight": 8
      },
      {
        "user": "admin",
        "pass": "admin",
        "weight": 7
      },
```


図-6 抽出したパスワードリストの出力例


```
{
  "table_init_func": {
    "tables": [
      {
        "id": 3,
        "type": "str",
        "str_data": "example.com",
        "table_addr": "080565d8",
        "refs": [
          {
            "func": "resolve_cnc_addr",
            "addr": "0804e552"
          }
        ]
      },
      {
        "id": 4,
        "type": "int",
        "int_data": 23,
        "table_addr": "080565e0",
        "refs": [
          {
            "func": "resolve_cnc_addr",
            "addr": "0804e5a9"
          }
        ]
      },
```


図-7 抽出したテーブルの出力例

*7 mirai-toushi(https://github.com/iij/mirai-toushi)。

・パスワードリストから検体が標的とする機器を推測
・C2サーバやScan Receiverのドメイン・IPアドレス・ポート番号をIoCとして活用
・新規のMirai亜種の検知

本ツールは1バイトXORの検体に対してのみ有効ですが、近年1バイトXOR以外の暗号化手法を利用する検体が登場しているため、このような検体への対応についても検討していきます。

1.5 おわりに

本稿では、2024年に注目されたセキュリティトピックを振り返り、DDoS攻撃を中心に観測情報や解析の取り組みについて紹介しました。

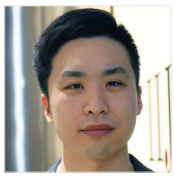
1年を通して重大な脆弱性情報が既に悪用された状態で報告される事案も少なくありませんでした。ランサムウェア攻撃では被害を受けた企業だけではなく、業務関係のある企業においても一部事業が停止するなどサプライチェーンを通じた影響を受ける事案が複数見受けられました。また、2024年末から翌年初頭にかけて、人々の生活に密着した企業を対象としたDDoS攻撃が相次いで報道され社会的にも大きく注目を集めています。第1.3節で紹介したとおり、IIJのSOCにて観測したDDoS攻撃の手法は従来から大きく変わっておらず、攻撃の送信元も依然としてルータやIPカメラなどのIoT機器が多い状況です。DDoS攻撃に加担するIoTマルウェアの感染は日本も例外ではなく、InfectedSlursに感染したと思われる送信元からの攻撃増加が確認されました。観測した攻撃の分析ではIoTマルウェアの解析も必要であり、クロスプラットフォームで展開されるIoTマルウェアの解析を効率化するため、第1.4節で紹介したmirai-toushiなどを用いた施策を講じています。

SOCでは引き続きDDoS攻撃をはじめとする脅威について情報分析基盤を用いた分析を継続し、そこで得られた情報を「wizSafe Security Signal」[*1]や小誌を通じて発信していきます。今後もセキュリティ対策や業務に役立てていただければ幸いです。

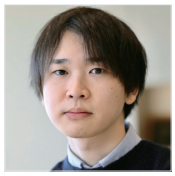
執筆者:

本部 栄成（ほんぶ えいせい）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

品田 祥太（しなだ しょうた）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課



森下 瞬（もりした しゅん）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課



西東 翔太（さいとう しょうた）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

リモートアクセスサービスの開発 ～IDゲートウェイの変遷～

2.1 はじめに

2024年9月末日、約26年間提供し続けてきた「IDゲートウェイサービス」がついに終了しました。1998年12月に開始[*1]し、IIJ史上最も長期に提供していたサービスの1つとなりました。

「IDゲートウェイサービス」は「リモートアクセス」を提供するサービスです。リモートアクセスは遠隔地のコンピュータに接続する技術で、今や広く普及しているリモートワークに必須の技術です。現在では、リモートアクセスには VPN技術が必須と考えられていますが、1998年のサービスリリース当初のIDゲートウェイサービスは、VPN技術を用いていませんでした。当時は拠点間のVPNでさえまだ普及の途上にあり、端末でVPNを行う実装は存在していましたが、実用的とはとても言えない代物でした。このような時代から、社会にとって必須の技術と言えるようになった現代に至るまで、IDゲートウェイサービスの歴史とともに振り返っていきたいと思います。

2.2 リモートアクセスサービスの始まり

IIJが「IDゲートウェイサービス」を開始した1998年ごろ、リモートアクセスといえば、Ascend MAXなどのダイアルアップ用のネットワーク機器を組織に設置し、そこに電話をかけ、PPPでIP接続することを意味していました。この場合のダイアルアップルータの意義ですが、インターネットに接続したいのならISPに接続することができるのですから、「内部につながる」ことが求められます。しかし、当時そういった機器は、ファイアウォールのようなアクセス制御ルールを書くことはできず、ほとんどなんの制限もなく内部のネットワークにつながっていたこともあったようです。

一方で、IIJは当時より内部ネットワークとインターネットは分離し、その境界にファイアウォールを置くことをユーザに推奨していたので、その裏口となるようなリモートアクセスは脆弱性そのものであり、IIJがサービスとして提供する場合には、リモートアクセスもまた、ファイアウォールと同様のアクセス制御ポリシーの中に収めるのが良いと考えました。また、ダイアルアップルータをユーザのネットワークに設置するのではなく、IIJのダイアルアップサービスを利用するよう設計しました。つまり、リモートアクセスのアクセス手段には既存のインターネットを用い、内部ネットワークへのアクセスにはファイアウォールのようなアクセス制御が必須であるという設計で、「IDゲートウェイ 1.0」は開発されました。

2.3 IDゲートウェイ 1.0

IDゲートウェイ 1.0は、アプリケーションレベルゲートウェイ型のファイアウォールをベースとして開発されました。ベースOSはBSD/OS 3.1でした。アプリケーションレベルゲートウェイ型のファイアウォールは、ファイアウォールを通過するすべての通信をプロキシが中断し、アクセス制御ルールに従い、許可する場合に限り以降の通信を中継するという動作をします。アプリケーションレベルで中継を行うため、HTTPやSMTPといったプロトコルを解釈して中継されます。このようなアプリケーションレベルゲートウェイ型のファイアウォールのアクセス制御部分を拡張し、PPPアカウントのユーザ名によって、宛先ごとに許可または禁止することを可能としました（図-1）。

このとき「ユーザを認証したのだから宛先はネットワーク全体に許可」というような大雑把なルールとならず、宛先ごとに許可することも多いと想定しました。それは、守るべき対象は接続ユーザだけでなく、宛先である組織内のサービスも守る必要があると、設計レビューや社内のβテストを通じて指摘されるようになったからです。きめの細かいアクセス制御を目指すことになりました。

＊1　「IDゲートウェイサービスを開始」、iij.ad.jp、IIJ（参照1998-10-02）（https://www.iij.ad.jp/news/pressrelease/1998/pdf/gateway.pdf）。

もう少し詳細を見てみます。図-2の左下からのユーザのアクセス要求は、オペレーティングシステムを通じて「中継プログラム」（プロキシ）に伝えられます。このときプログラムにはユーザのソースIPアドレス、宛先のIPアドレスとポート番号が伝わり、中継プログラムはその通信がアクセス制御ルールにより許可されているものかを「ID認証デーモン」に問い合わせます。アクセス制御ルールはLink-ID（PPPアカウントのユーザID）で記述されているため、ID認証デーモンは、ソースIPアドレスからLink-IDへの変換が必要となります。ID認証デーモンは、前回の問い合わせがキャッシュとして存在すればそれを用いて直ちにソースIPアドレスからLink-IDへの変換を完了します。キャッシュに存在しない場合、「IDサーバ」と呼ばれるIIJのサーバに問い合わせを行います。ID認証デーモンとIDサーバ間の通信には「Link-IDプロトコル」というIIJで開発した独自プロトコルが利用されました。

Link-IDを得たID認証デーモンは、アクセス制御ルールと照らし合わせ、当該ユーザに対してアクセスが許可されているかどうかを判定し、許可/不許可を中継プログラムに返却します。これにより、アクセス制御ルールで許可されたリモートアクセスのみを許可することを実現しました。

2.4 IDゲートウェイ 2.0

2000年9月にリリースした「IDゲートウェイ 2.0」では、コンソールアプリケーションだった設定ユーザインタフェースを、「IDゲートウェイポリシーマネジャー」というグラフィカ

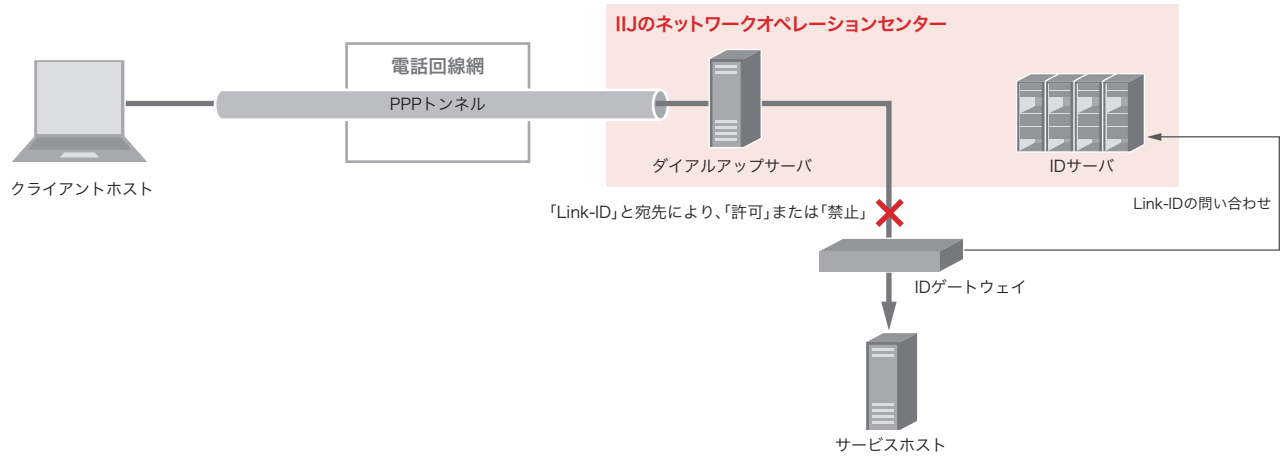


図-1 IDゲートウェイ1.0の全体構成

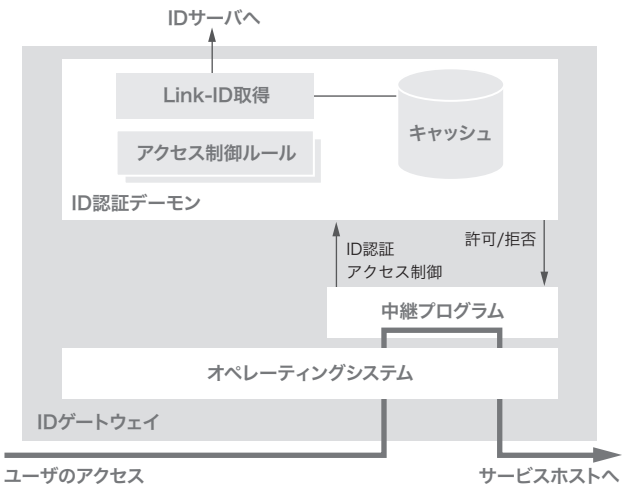


図-2 IDゲートウェイ1.0のアクセス制御

ルユーザインタフェース(GUI)に一新しました。アクセス制御ルールを設定するためのアクセス制御ルールパネルは、アクセス制御ルールを分かりやすく設定してもらうにはどうしたら良いか議論を重ねた結果、最終的に図-3のように、スプレッドシートに○×を付けていくユニークなものとなりました。また、ベースOSもNetBSD1.4に変更されています。

2.5 IDゲートウェイ 3.0

2002年4月にリリースした「IDゲートウェイ3.0」では、ついにL2TP/IPsec、PPTPといったPPPをベースとしたVPN接続をサポートします。しかし、当時この実現にはいくつもの壁を乗り越える必要がありました。

まずL2TPやPPTPといったトンネリングプロトコルを実装する必要がありました。当時、既存のオープンソースの実装は1トンネルごとに1プロセスを用いるプロセスフォーク型の実装で、この場合IDゲートウェイサービスの想定する規模ではプロセス数が数百となり、メモリを逼迫して利用することができません。IDゲートウェイ上のデーモンは1.0当初よりイベントドリブン型で実装していましたが、トンネリングプロトコルもイベントドリブン型で実装する必要がありました。実装はC++で、ゼロから行いました。

続いてL2TP/IPsecのIPsecの部分ですが、WIDEのKAMEプロジェクト*2のIKEやIPsecの実装がNetBSDに取り込まれ、それを用いることができました。ただし1つ問題がありました。NAT越しにIPsecを利用するためにはIPsec NAT-Tを実装する必要があるのですが、NetBSD 1.4に取り込まれたバージョンにはその実装はありませんでした。IPsec NAT-Tを実装しない場合、まずUDPチェックサムが一致せず、それを回避してもNAT配下の1ホストしか接続できない問題が発生します。IDゲートウェイサービスでは、それを「先着一名問題」と呼んでいました。IDゲートウェイ 3.0では、先着一名問題は制限事項とし、UDPチェックサムが一致しない問題のみを解決することとしました。UDPチェックサムの問題は、受信時はESPのHMACによる確認があるのでUDPチェックサムの確認はスキップできるとして、スキップするようにしました。一方、送信時はオプショナルであるUDPのchecksumフィールドを0にして利用しないこととし、対向ホストでもチェックサムの確認がスキップされるようにしました。

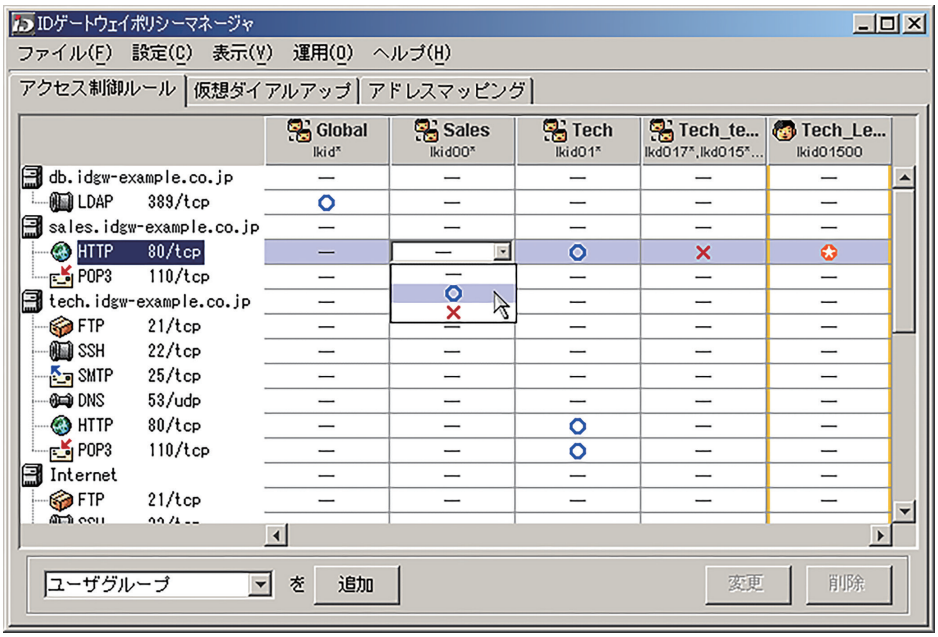


図-3 IDゲートウェイ2.0のポリシーマネジャー

*2 KAMEプロジェクト(https://www.kame.net/index.html)。

PPTPについても、NAT越えで問題が発生する可能性があります。PPTPは、コントロール部分はTCPを、データ部分はGREを用います。コントロール部分はTCPであるためNAT越えの問題は発生しませんが、データ部分のGREはL2TP/IPsec同様に問題が発生する可能性がありました。ただし、GREヘッダのCall-IDを用いてNATマスカレードを行う実装が、コンシューマルータを中心に普及し始めていました。このため、L2TP/IPsecよりもPPTPの方が「先着一名問題」が起こりづらいと考えました。また、PPTP ではパケットの暗号化にMPPEを用いることが事実上必須で、MPPEはプロプライエタリな暗号アルゴリズムであるRC4を利用します。このため、RSA Data Security社とのライセンス契約を行って使用許諾を得ました。

PPP部分の実装はiij-ppp[*3]をベースとした FreeBSDのpppが、Multi-PPPという複数の回線に複数のPPPを確立させるための拡張を行った結果、1プロセスで複数のPPPを終端できるようになっていたため、元々IIJ が開発していたものでもあり、これを利用しました。

また、VPNの認証はどうするのかという課題もありました。通常のVPNサービスならば、まずはユーザのディレクトリサービスに接続して認証することを考えますが、IDゲートウェイの場合、2.0まではダイアルアップ接続をしていたのですから、既存のユーザはIIJのダイアルアップサービスを契約しており、接続ユーザにはPPPアカウントを発行済みで、アクセス制御ルールもそのアカウントで設定しています。VPNの認証もそのアカウントで行うことにすれば、既存のいろいろな部分が共通で利用できると考え、そのように実装しました。IDゲートウェイ上のPPPデーモンの認証リクエストは、ID認証デーモンによりプロキシされ、IIJのIDサーバ上のRADIUSサーバにて認証が行われる仕組みとしました。これにより、利用ユーザは同一のPPPアカウントを、ダイアルアップにも、VPNのL2TP/IPsecやPPTPのエントリにも、同じように設定することができました。アクセス制御の仕組みも図-4のように、従来とほとんど変わらない仕組みで実装することが可能になりました。このように従来のダイアルアップと同じようにVPNを扱えるようにしたため、IDゲートウェイサービスの中ではこれを「仮想ダイアルアップ」(VDIP)と呼び、従来のダイアルアップを「実ダイアルアップ」と呼ぶことにしました。

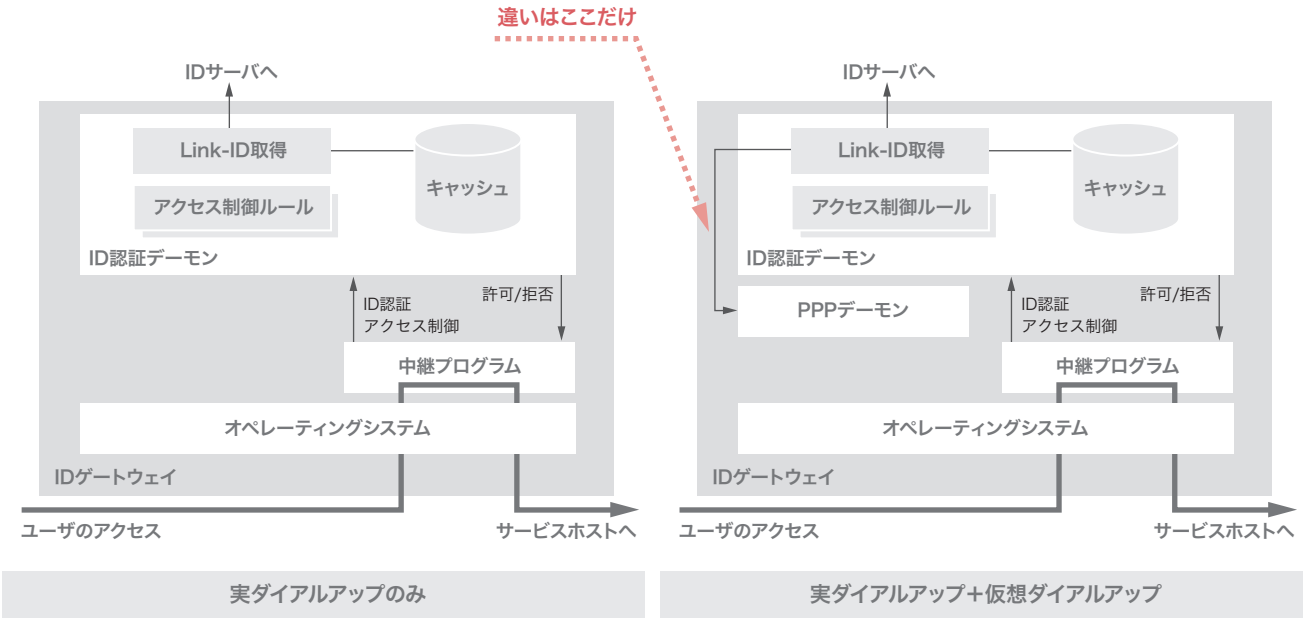


図-4 ダイアルアップ方法とアクセス制御

*3　IIJの大野らが開発したオープンソースのPPP実装。1990年代後半から2000年代前半にはBSDユーザを中心に広く利用された。

2.6 IDゲートウェイ 4

2005年7月にリリースした「ID ゲートウェイ 4.00」では、「認証サーバ連携」機能を追加し、仮想ダイアルアップの認証サーバとして、Active Directoryなどのユーザ側ネットワークの RADIUSサーバやLDAPサーバを利用できるようにしました。また、リポートシステムを一新し、ルールビューア機能も追加しました。

2006年4月にリリースした「IDゲートウェイ 4.02」では、「SSLダイアルアップ」(SSLDIP)という新しいVPNプロトコルを実装しました。L2TP/IPsecやPPTPは、既に触れたようにNAT越しに利用した場合に問題が発生することがあります。また、制限された組織内のネットワークや海外のホテルなどからはHTTP、HTTPS、DNSなどの限られたポートしか許可されていないために、まったく利用できない場合もあります。一方で当時、SSL-VPN製品が市場に出始めており、SSLをトランスポートとするSSL-VPN製品はこういった問題がまったく発生しないため、IDゲートウェイにも同等の機能の実装が求められました。

SSLDIPはSSL(現在のTLS)をトランスポートにし、クライアントとIDゲートウェイ間でL2トンネルを作成し、その上でPPTPを行う設計としました。この狙いは、最終的なトンネルをPPPベースに揃えることで、その他の仕組み、認証やアクセス制御は従来と同一の仕組みが使えるようにすることでした。L2トンネルはオープンソースのOpenVPNを利用することにし、設定や接続管理を容易にするWindows用のクライアントも開発しました。

この他、IDゲートウェイ 4.02では、L2TP/IPsec、PPTPサーバ機能の実装をゼロから書き直して新しいデーモンにしました。元の実装は、VPNのトンネル処理部分がCではなく、C++で書かれており、SEIL(IIJ独自開発の企業向け高機能ルータ)シリーズ[*4]など組み込みの環境への移植に問題がありました。また、従来はPPP部分は別のプログラムでしたが、これも必要最小限のシンプルなものに書き直し、それをVPNと同じプログラムに組み込んでしまうことで、性能向上や保守性の向上を狙いました。このプログラムがnpppd[*5]で、後にOpenBSDに取り込まれるものです。また、RADIUS部分は元々IDサーバで利用していたコードを流用したものでしたが、それが現在のOpenBSDのRADIUSライブラリ[*6]の原型となりました。

2.7 IDゲートウェイ 5

2008年3月にリリースした「IDゲートウェイ 5.00」では、「端末認証」機能を追加しました。VPN接続時の認証の他に追加の認証を行うもので、現在は「多要素認証」と呼ばれているものに相当します。「接続端末を限定したい」「パスワード漏えいに備えたい」といった要望に応える機能でした。IDゲートウェイの「端末認証」機能は、VPN接続後、端末認証を実施するまでは、DNSと認証ページにしかアクセスできないよう制限され、端末認証が成功すると、本来のアクセス制御ルールに切り替わる仕組みで、ID認証デーモン及び中継プログラムを機能拡張しました。このアクセス制限の仕方は、現在「キャプティブポータル」と呼ばれるものに相当します。認証の仕組みは、クライアントからのWebアクセスを認証ページに誘導した上で、認証ページ内のアプレットによりクライアント端末のMACアドレスをIDゲートウェイに送信させ、IDゲートウェイ上のデータ

＊4　SEIL(https://www.seil.jp/)。
＊5　src/usr.sbin/npppd/、github.com、GitHub(https://github.com/openbsd/src/tree/8b2d863473/usr.sbin/npppd/)。
＊6　src/lib/libradius/、github.com、GitHub((https://github.com/openbsd/src/tree/8b2d863473/lib/libradius/)。

ベースにより、あらかじめ登録済みのMACアドレスと一致するのかを照合することで、VPNの認証ユーザが所有する正規の端末からの接続であることを確認する仕組みとしました。

この他、ホットスタンバイを実現するVRRP機能をSEILから移植する形で追加しました。また認証サーバ連携機能でEAP認証の利用をサポートしまた。

2009年12月にリリースした「IDゲートウェイ 5.02」では、オペレーティングシステムのソースコードをSEIL/Xシリーズのソースコードとコードベースを統一しました。これにより、IPsec NAT-Tが有効となり、長年の課題であったNAT配下で複数のユーザがL2TP/IPsecを利用できなかった問題が解消されました。ベースOSは NetBSD 3.1に変更されました。

2.8 IDゲートウェイ 6

2011年11月にリリースされた「ID ゲートウェイ 6.00」では、新しいトンネリングプロトコルとしてSSTPをサポートしました。SSTPはMicrosoftが開発したTLS上で動作するプロトコルで、L2TP/IPsecなどと同様に、PPPフレームをトンネリングします。TLSベースであるため NAT配下からの接続時の問題もなく、クライアントもWindows標準に含まれるため、IIJ独自のクライアントを配布する必要がありません。また、PPPベースであるために認証部分やアクセス制御部分はそのまま流用することができます。SSTPは公開プロトコルであるものの、商用利用にはMicrosoftの使用許諾が必要で、契約を結びました。

2.9 IDゲートウェイ開発の終息と課題

仮想ダイアルアップを開始した当初の技術課題であったNAT配下からの接続時の問題も、5.02のIPsec NAT-Tのサポートと、6.00のSSTPのサポートをもって解消しました。しかし一方で、ユーザ1人当たり負荷は年々増加傾向で、要求される性能を1台では処理できないという状況が発生してきました。

まず要因として挙げられるのは、IDゲートウェイは当初よりアプリケーションゲートウェイのソフトウェアでありルータではなく、すべての通信はアプリケーションレイヤーで中継しており、基本的にIP転送は行っていないことです。IPレベルで転送する場合と比べ、どうしても負荷は高くなるのです。ケースバイケースでIPレベルでの転送にオフロードするような仕組みを持つべきでした。

次に要因として挙げられるのは、アプリケーションゲートウェイを提供する中継プログラムのソフトウェアがシングルプロセスで動作する設計であるため、CPUが複数あっても活用できない問題、マルチコア対応に問題がありました。

最後に要因として挙げるのは、ベースOSのカーネルです。IDゲートウェイの最後のバージョンのベースOSはNetBSD 3.1ですが、ネットワークスタックのマルチコア対応は未着手で、中継プログラム同様、CPUが複数あっても活用できない問題、マルチコア対応に問題がありました。

これらの問題は個別の問題のようでいて、実はソフトウェアの陳腐化の表れに過ぎないと考えています。現在のソフトウェ

アはインターネットを通じてグローバルに進化を続けるものなので、放っておけば常に陳腐化していく宿命にあります。IDゲートウェイのソフトウェアの問題は、このようなソフトウェアの陳腐化について無策であったことだと振り返っています。

これらの課題をIDゲートウェイの延長として解決することは、様々な面で困難であると判断し、後継サービスである「IIJ GIO リモートアクセスサービス」と、「Tornado」という新たなIIJ内製のゲートウェイOSに役目を引き継ぎ、IDゲートウェイのソフトウェア開発は終息することにしました。

2.10 IIJ GIOリモートアクセスサービスとTornado

2013年2月、IIJ GIO リモートアクセスサービス(GAM)という新たなリモートアクセスサービスを開始しました。GAMはクラウド型のサービスで、VPNのゲートウェイはIIJのクラウド上で動作しています。VPNゲートウェイには、IDゲートウェイに代わり新たにIIJ内で開発していたTornadoを利用しています。

TornadoはIIJ内のネットワーク系のソフトウェアを機能統合するIIJ内製のゲートウェイソフトウェアで、OpenBSDをベースに開発しています。IDゲートウェイの後継となるような製品を作るためにベースOSに求められるのは、企業のファイアウォールとして利用可能なレベルのパケットフィルタ機能、透過プロキシのためのカーネル拡張が行えることですが、OpenBSDは開発開始当初の2011年時点でこれらすべてを実現可能でした。むしろ、アプリケーションでの中継処理からカーネル内の処理に戻すソケットスプライス機能や、ポリシールーティングなどを実現するVRF機能など、IDゲートウェイにも欲しかった機能が最初から利用可能でした。また、IDゲートウェイ由来のnpppdも取り込まれていました。

Tornadoでは、中継プログラムはマルチコア対応の新しいデーモンに差し替えました。また、アクセス制御ルールにおいて、アプリケーションレベルで中継するか、パケットフィルタによりIPレベルで転送するかは、単に1つの設定項目として切り替え可能としました。

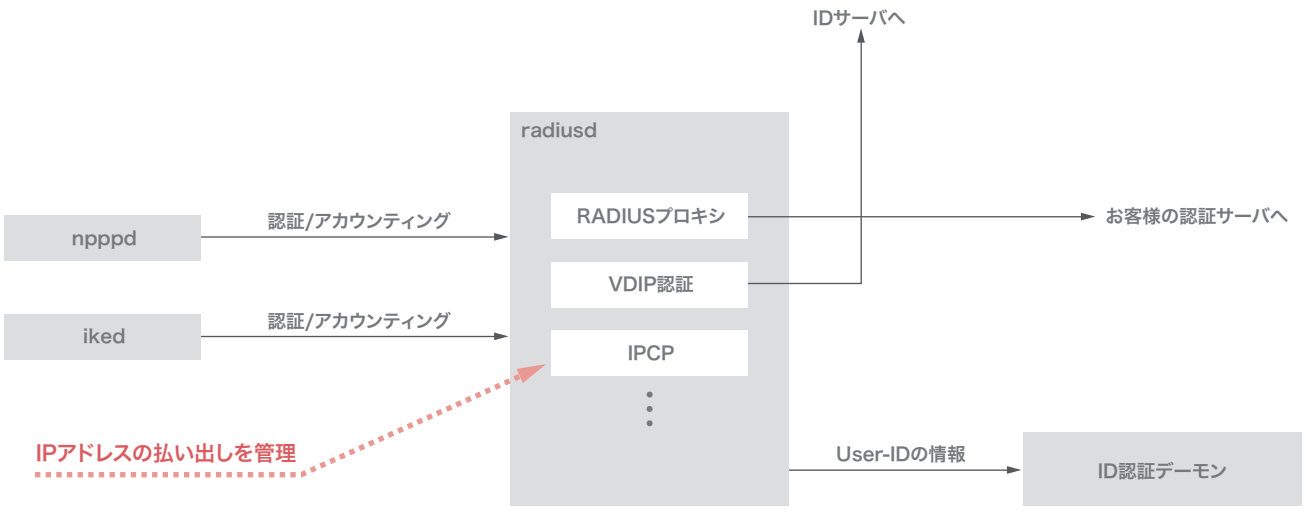


図-5 IKEv2を用いた接続の全体構成

IDゲートウェイとTornadoの大きな違いとしては、IDゲートウェイはIDゲートウェイサービス専用のソフトウェアだったのに対し、Tornadoは汎用のソフトウェアである点です。サービス固有で共通化できない機能は、オプショナルなパッケージとして開発する設計となっています。サービス固有の機能は、比較的代謝が激しく、常に新しいものが求められ、古いものは廃れていく傾向があります。こういったものを取捨しやすい設計としました。

2024年12月、GAMでは、新たなVPNプロトコルIKEv2による接続をサポートしました。IKEv2はPPPベースのプロトコルではないため、当時のOpenBSDのIKE v 2のデーモンでは認証やアクセス制御の仕組みが他のプロトコルのものを流用できませんでした。この問題を解決する際、PPPベースのものとまったく別の仕組みを作ってしまうと、2つの別々の方法を管理保守していくことになります。Tornadoでは、IKEv2のデーモンにRADIUS認証及びアカウンティング対応を機能追加することで、仕組みを共通化することにしました。認証をRADIUSにして一元化し、それだけでなく、図-5のようにローカルのRADIUSデーモンがVPNに払い出すIPアドレスを一括して管理することにより、PPPベースのVPNもIKEv2も同じようにアクセス制御の仕組みが動作するように実装しました。

内部ではTornadoバージョン 4.5が利用されますが、これは約1年前にリリースされたOpenBSDをベースOSとしており、比較的新しいバージョンを利用できていると言えます。IDゲートウェイの反省から、継続的インテグレーションとして、定期的にベースOSのバージョンを更新し続けているため、ベースOSが古いバージョンで停滞することはなくなりました。

2.11 まとめ

振り返ってみると、IDゲートウェイは当初より単なるリモートアクセスを提供するサービスではなく、PPPアカウントにより認証し、その認証IDに対してアクセス制御ルールで許可された通信だけが行える、といったセキュリティ機能を提供していました。また、IDゲートウェイ 5でデバイスレベルの認証を加えました。これらは、現在でいうZero trust architecture（ZTA）の考え方そのものです。

IDゲートウェイからIIJ GIOリモートアクセスサービスへの歴史は、IIJ内製のソフトウェアの開発の歴史でもありました。TornadoはIDゲートウェイを引き継ぐ現在進行形のIIJの基盤ソフトウェアです。今後も新たな技術に取り組んでいくことはもちろん、ユーザのニーズの変化、社会情勢の変化にも対応してより良いサービスを提供できるよう尽力していきます。

執筆者：
保岡 昌彦（やすおか まさひこ）
IIJ ネットワーク本部 システム技術開発部
1998年入社。IDゲートウェイなどを開発したのち、IIJ内製のソフトウェアを機能統合するゲートウェイ OS "Tornado" を立案し開発、現在も開発、保守を行っている。

Information

1. 未来のネットワーク社会を担うトップエンジニア育成の場「IIJアカデミー」

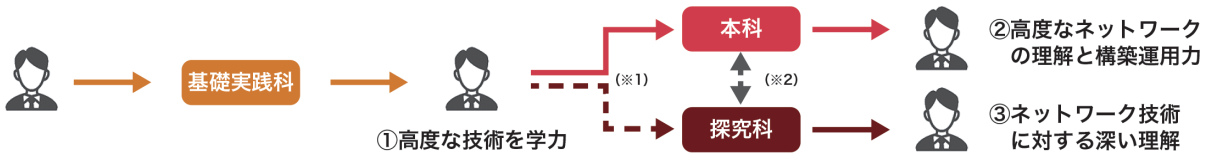
「IIJアカデミー」は未来のネットワーク社会を担うトップエンジニア育成のため、2023年にIIJ創業30周年を記念して開設されました。IIJが創業以来培ってきたインターネットサービス開発・運用の知見をベースに、実践的な知識・スキルを習得できる学びの場を提供し、未来のネットワーク社会とIT産業の根幹を支える高度な技術を持つIT人材を育成することを目指しています。

このたび、第5期（2025年5月12日～2025年9月5日）の受講生募集を開始しました（募集期間は4月7日（月）正午までの予定）。また、第6期を11月上旬開講（2025年9月上旬より募集開始）予定です。

第5期では、IIJアカデミーの中心的な実習プログラムである「本科」の受講につながる基礎的なネットワーク技術を習得する「基礎実践科」を新設するとともに、「探究科」に新たにカリキュラムを追加し、実習プログラム体系を拡充しました。また、これまで16週間で実施していた「本科」を前半・後半それぞれ8週間に分割し、希望するカリキュラムを単体で、受講者のスケジュールにあわせて効率よく受講できるよう実習期間を改定しました。

■ IIJアカデミーの実習プログラム体系

ネットワーク・システムの中核となる技術の習得を目指す「本科」と、個別の技術テーマの理解を深める「探究科」、またIIJアカデミーの中心的な実習プログラムである「本科」の受講につながる基礎的なネットワーク技術を習得する「基礎実践科」の3つの実習プログラムを提供しています。



(※1)本科・探究科はどちらからでも受講可能ですが、中心的なカリキュラムである本科から受講を始めることをお勧めします。
(※2)本科・探究科の双方を受講することで、ネットワーク運用におけるより一層高い実践力を身に付けることができます。

＜カリキュラム受講後の人材像＞

① 高度な技術を学ぶ力を持った人材
高度なネットワーク技術の学習のために必要な、ネットワーク機器の設定や状態確認、パケットの観察方法などの技能を身につけた人材

② 高度なネットワークを理解し、構築運用ができる人材
複雑なルーティングや確実な冗長化など、商用レベルで用いられる技術が適用されたネットワークの構築運用が行える人材

③ ネットワーク技術に対する深い理解を持った人材
プロトコルの設計や、その背景にある思想・経緯を理解し、実際のネットワーク上で発生している現象を読み解くことができる人材

＜カリキュラム一覧＞

【本科】
[前半] クラウド基盤のためのデータセンターネットワークの設計と構築
[後半] 動的経路制御を用いたネットワークの設計と構築

【探究科】
[前半] TCP輻輳制御アルゴリズムの比較検証
[後半] traceroute コマンドを自作する

【基礎実践】★5期より新設
オフィスネットワークで学ぶITC/IP入門

カリキュラムの詳細や募集要項はIIJアカデミー公式サイトにてご案内しております。
募集期間等は変更する可能性があります。
最新の情報は当サイトにてご確認ください。

IIJアカデミー
公式サイト

2. IIJ公式エンジニアブログ 連載「運用の現場から ～ ICT社会を支えるために」

ITシステムやインターネットで避けられないこと――それは機器の故障やトラブルです。
世の中にあるシステムのほとんどは、なにもしていないと壊れます。それを動かし続けるための営みが「運用」です。

IIJが提供する通信・クラウド・セキュリティなどのサービスは、多くの企業でシステムの一部として利用されています。そうしたシステムが安定して稼働できるように、IIJはサービスの運用に力を尽くしています。

さて、一口に「運用」といっても、様々な要素があります。
例えば、

- 運用が適切に行えるような、システム・ネットワーク設計
- サーバや通信機器の稼働状況を把握する、監視とモニタリング
- 故障部品の交換や、ソフトウェアのアップデート作業の計画と実施
- お客様サポート、社外のエンジニアの皆さんとのコミュニケーション
- それらの作業を下支えする、蓄積された経験と最新の情報収集

これらの要素が集まることで、高い運用品質が保たれています。

IIJ公式エンジニアブログでは、運用にまつわる活動を様々な部署で働くエンジニアが紹介しています。ぜひご覧ください。

IIJ公式
エンジニアブログ
「運用」特集

■ IIJ 公式Xアカウント@IIJ_ITS

なお、各媒体の記事公開やイベント開催情報は、IIJ公式Xアカウント@IIJ_ITSでお知らせしています。ご興味のある方はぜひフォローしてください。

@IIJ_ITS　https://x.com/IIJ_ITS/

March 2025 Vol.66

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本冊子の情報は2025年3月時点のものです。

IIJ-MKTG019-0066

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp