IIJ. news

IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan.
Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry.
The history of IIJ is indeed the history of the Internet in Japan.

April 2022
VOL. 169

特集

セキュリティのトレンド 2022 Spring

IIJ. news
April 2022
VOL. 169

ぷろろーぐ

行事は消えて

株式会社インターネットイニシアティブ
代表取締役会長
鈴木 幸一

最近は、季節の移り変わりを象徴する行事や儀式が次々と消えているが、新型コロナウイルス対策など、さまざまな規制を盾にその傾向がますます強くなっているようだ。

子供がある年齢になると、育った家を出て、別の場所で暮らすようになる。それぞれがバラバラに住むようになると、家族は小さくなって、墓参りをはじめ、家庭で何代も引き継がれてきた行事が当然のようになくなっていく。

高校を卒業してすぐ、横浜の中心にある実家を出てしまった。東京まで小一時間なのになぜ家を離れたのか、記憶が遠くなり過ぎて、理由は覚えていないのだが、以後、何十年も地面と接点のない部屋で暮らしている。育った家で、折々の季節ごと、手間をかけて、形にしていた行事もほとんど忘れてしまった。

明治生まれの両親に育てられたせいか、五節句――人日（一月七日）、上巳（三月三日）、端午（五月五日）、七夕（七月七日）、重陽（九月九日）には、お祝いの料理などを食べた記憶がある。今、私がささやかな行事としているのは、端午の節句に菖蒲湯を楽しむくらいである。マンションの浴室では、菖蒲湯に浸かっても、端午の節句を祝う気分には、およそなれないのだが、それでも昔のことを思い出すきっかけくらいにはなる。

近年はパンデミックの影響もあって、入社式もネット上で行なっていたのだが、今年は三年ぶりに新入社員がオフィスに集まり、昔ながらの形で行なわれた。男子は紺のスーツと白いワイシャツ、ストライプのネクタイ、女子は紺のスーツに白いブラウス、誰もが同じ服装である。儀式なのだからそれらしい雰囲気が出るようにと、新入社員一同の考えなのだろうが、ネクタイを締めているのは私だけだったIIJはどこに行ってしまったのだろうと、余計な心配をしてしまう。

些少な資本しか持たないなかIIJを設立したのは一九九二年で、今年で三〇周年になる。インターネットを知る人もいなかった時代、情報通信という巨大な資本を必要とする事業で成功するはずがないと、私の親しい友人ですら、関心といえば、いつまでもつのかという危惧しかなかった企業が、なんとか三〇周年を迎えて、大企業の入社式のような雰囲気である。

「ネクタイを締めろとまでは言わないけど、せめてひとりくらい、ジャケットを着てもいいと思わない？」。新入社員の採用を始めた頃、一緒にIIJを立ち上げた友人に呟いたら、「いつ夜逃げするのだろうと思われている零細企業に、バリッとした服装で集まったら、それこそ可笑しいよ」。そう言われて、ようやく解体寸前のビルから引っ越したばかりの企業に、ネクタイを締めた背広姿の新入社員が集まる光景のほうが、アンバランスで奇妙だと思いながら、煙草をふかしていた。

「ともかくインターネットに関わりたい。IIJ以外にインターネットに関われて、尊敬できる技術者がいる場がないから」。IIJで働く気になった動機を聞くと、たいていそんな答えが返ってきた。当時、怪しげな身なりをして、昼夜を分かたず働き詰めだった若者も還暦近くになっている。月日が過ぎてしまうと、時間に対してまったく別な思いが湧いてくる。せめて、なにか行事をつくってみようかと思うのだが。

イラスト／末房志野

TOPICS

セキュリティのトレンド 2022 Spring

「セキュリティのトレンド 2022 Spring」と題した今回の特集では、
近頃、インターネットの脅威動向に関する情報から少し遠ざかっている方や、
この春、初めて情報システムやセキュリティ関連のお仕事に就く方を対象に、
知っておくとよいトピックをやさしく紹介していきます。

本論に入る前に、まずはご自身の「最近のセキュリティ・トピックスに関する知識」を
左ページの全４問からなるクイズで確認してみてください。
答えがわからなかった方は、各論をご一読いただき、
セキュリティに関心をもっていただけたら幸いです。
全問正解の方は、社内のセキュリティを牽引する立場でご活躍されることと思います。

特集イラスト／高橋 庸平

セキュリティ・ナレッジをチェックしよう！

Q1

手を変え品を変え、
メールで攻撃を仕掛けてくる悪質な行為に対し
「半永久的に有効な対策」はあるでしょうか？

① 現時点ではない。しかし、メールセキュリティに関する情報収集と対策を継続的に行なうことは、被害を少なくするために重要である。

② 現時点ではない。しかし、メールセキュリティを検討する国際的なコミュニティに参加し、日頃から知見を蓄えている企業が開発したメールセキュリティサービスを導入することは、一つの対策になり得る。

③ ある。メールの利用を社内・社外ともに撤廃して、電話やFAXなどのコミュニケーション手段に切り替える。

Q2

家庭内にあるIoT機器が、
気づかぬうちに悪意ある攻撃者に利用され、
DDoS攻撃の踏み台として使われる事例が発生しています。
これを防ぐためにできることは、次のうちどれでしょう？

① 機器を初期設定のID／Passwordで使わない。

② 機器のファームウェア・ソフトウェアを最新版にアップデートする。

③ メーカによるアップデート、メンテナンスが終了した機器は早めに交換する。

Q3

インターネットが送信先となるDDoS攻撃が、
結果的にIIJバックボーンで
輻輳を引き起こすことがあります。
この事象を端的に言い表す「ことわざ」は
どれでしょう？

① 塵も積もれば山となる。

② 弘法も筆の誤り。

③ 船頭多くして船山に上る。

Q4

Apache Log4j の脆弱性である Log4Shell の
情報が昨年12月に公開されました。
攻撃者はなぜ Log4Shell を悪用するのでしょうか？

① 攻撃が容易であるため。

② 攻撃の影響を受けるソフトウェアが多いため。

③ 脆弱性への対策が不十分な環境が多くあるため。

A1 ①と②
A2 全て
A3 ①
A4 全て

メッセージングセキュリティの第一歩

リモート環境での活動にメールの利活用は欠かせない。
しかし、そうした状況を逆手にとった攻撃も増えている。
ここでは、メールをめぐるセキュリティについて考えてみたい。

IIJ ネットワーク本部 サービス推進部
櫻庭 秀次

便利な環境が格好の標的に

コロナ禍により社会環境が変化し、リモート環境での作業やコラボレーションが進んでいます。こうしたタイミングでさまざまな場所からインターネットに接続できる環境がある程度整ってきたことは、社会活動の継続のための有益なツールとして活用されていると同時に、インターネットが重要な社会基盤となっていることを実感する部分でもあります。しかしながら、インターネットの利用者や接続する機器が増えれば、それらを狙うような攻撃行為も増えてきます。

有名ブランドなどを騙って偽のサイトに誘導し、ログイン情報や金銭につながるような個人情報を摂取する**なりすましメール**（フィッシング詐欺）が引き続き高い頻度で続いています。最近では、マルウェア（不正プログラム）に感染させることで、PCに保存されている情報を摂取したり、それらの情報を悪用して新たなマルウェア感染者を増やすといったなりすましメールも急増しています。ほかにもファイルを暗号化して解読と引き換えに金銭を要求するランサムウェアなど、その手口や対象も広がっています。特にランサムウェアは、暗号化されたファイルが顧客の個人情報など重要なものであった場合、支払いに応じなければインターネット上に公開すると脅迫するなど、より悪質化しています。また、重要なデータが暗号化され参照できなくなってしまうことで、業務遂行に影響をきたし、経営上の問題にまで発展する可能性もあります。

メールは組織内部に直接情報を届けることができるほぼ唯一の手段であり、多くの組織で利用されています。届ける情報も、単なるテキストメッセージだけでなく、添付ファイルのようにPCで実行可能なプログラムなど、多様なデータを運ぶことができます。PC利用者間でのデータも共通化され、相互利用できるようになりましたが、そうした便利な環境は、マルウェアやそれへの感染を促すデータの送信者にとっても都合が良い環境となっています。

コミュニティへの参加が対策の第一歩

悪意な行為を行なう側は、ビジネス（金銭）が目的なので、特定の手法に対する対策を講じたとしても、また新たな手法を生み出して攻撃を続けてきます。どこまで対策すればいいのか聞かれることもありますが、残念ながら、先を見通した完全な対策を現時点で講じるのはむずかしいでしょう。将来的にも有効な対策があったとしても、それは使い勝手の面で問題があったり、制約が強すぎてインターネットの可能性を狭めてしまう対策であるかもしれません。

とはいえ、なるべく被害を受けないよう、状況を確認しつつ、何かあった場合には、素早く対策を講じていくことは必要かつ可能です。新たな手口は世界のどこかで試みられているため、そうした状況をいち早く把握し、その危険性や対策を察知・検討するためにも、グローバルなコミュニティに参加して情報共有や互いの知見を出し合うことも重要です。

例えば、メッセージングセキュリティの分野においてIIJは、M3AAWG*に創設時から参加しています。ここでは、なりすましメール対策に関する標準的な技術仕様の発端や思いつきレベルの発想（笑）まで、さまざまなアイデアを持ち寄って議論しています。M3AAWGには多くのサービス運用者も参加しており、新しく導入を予定している対策やその後の状況を知る機会にもなっています。そして、そこでの成果がIIJのサービスにも反映されています。

メッセージングセキュリティの分野で、こうした活動とサービス提供の両方を実践していくことは相乗的な効果もありますが、リソース面などで簡単ではありません。全ての組織が同じような活動をすることはむずかしいので、できる範囲で活動に参加し、状況を把握して適切な対応が何かを理解していくことが大事です。

IIJはインターネットの主要なサービスを長く提供してきたと同時に、国内外の多くのコミュニティに積極的に参加してきた経緯があります。今後も安心・安全なサービスを提供するために、こうした活動を継続していきます。

＊M3AAWG：Messaging, Malware and Mobile Anti-Abuse Working Group　https://www.m3aawg.org

IoT機器の設定を確認しよう！

身近な機器といえども、インターネットにつながっていると、
悪意のある攻撃に狙われる恐れがあるため
IoT機器の設定確認は不可欠である。

IIJ セキュリティ本部 セキュリティ情報統括室
土屋 博英

設定確認の重要性

インターネットを介した多様なサービスを手軽に利用できるようになりました。PC、タブレット、スマートフォンだけでなく、スマートスピーカー、ネットワークカメラ、連携機能を持ったスマート家電といった「IoT機器」を使われている方も多いと思います。

生活を豊かにしてくれる便利な機能を手軽に使えるようになった反面、IoT機器の管理・設定の不備や脆弱性（ソフトウェアの不具合）を狙った悪意のある攻撃も多発しています。攻撃はインターネット上で無差別に行なわれており、誰でも被害を受ける可能性があります。これらの攻撃を受けた機器が次の攻撃に悪用されることで、加害者となってしまう危険性もはらんでいます。

IIJのお客さまのなかにも攻撃を受けて、**DDoS攻撃**の踏み台になってしまったといった事例が発生しています（次頁「IoT機器を介したDDoS攻撃発生の仕組みとバックボーンへの影響」参照）。そうしたお客さまに利用環境を確認すると、ルータなどのネットワーク機器だけでなく、ネットワークカメラやNAS*などの機器が踏み台にされ、別の攻撃に悪用されている事例が多いことがわかります。

利用者は家のなかでのみ使っているつもりでも、設定によっては、インターネットに公開している状態になっており、不特定多数からカメラの映像をのぞき見されたり、プライベートなファイルを期せずして公開してしまっているといったケースもあり得ます。

例えば、スマートフォンのアプリを介して、外出時にも機器を遠隔操作できるものがありますが、設定状況によってはインターネットを通じて、正規の通信だけでなく、悪意のある攻撃を目的とした通信を受けてしまう危険性もあります。

これらを防ぐには、利用している機器の設定が安全かどうか、適切に確認する必要があります。確認するポイントを挙げると――

- IDやパスワードが初期設定のまま機器を使っていないか確認する。
- 利用している機器のファームウェアやソフトウェアが最新版にアップデートされているか、メーカのサイトなどで確認する。
- 覚えのない設定が入っていないか、インターネットから制限なく接続できる設定になっていないか確認する。
- 覚えのない機器や想定していない機器が接続されていないか確認する。

一部のブロードバンドルータでは、ネットワークにつながっている機器の一覧を表示してくれるものもあります。こうした機能を使うなどして、普段からネットワークにつながっている機器を確認しておきましょう。

機器の買い替えも視野に

機器によっては、メーカによるアップデートやメンテナンスが行なわれなくなったものもあるかもしれません。このような機器は今後、悪用される可能性が高いため、利用の停止や新しい製品に買い替えるといった対応が必要になります。まだ使えるから、壊れていないからといって使い続けるのではなく、利用している機器を定期的に確認し、安全性を見直すことも利用者が考えなければならない対策です。

最近では、セキュリティ的に問題のある設定は、出荷時にオフになっていたり、自動的にソフトウェアを更新する機能がついている機器も増えてきました。新しく購入する際は、そうした機能やサポートがしっかりしている製品を選ぶよう心がけましょう。

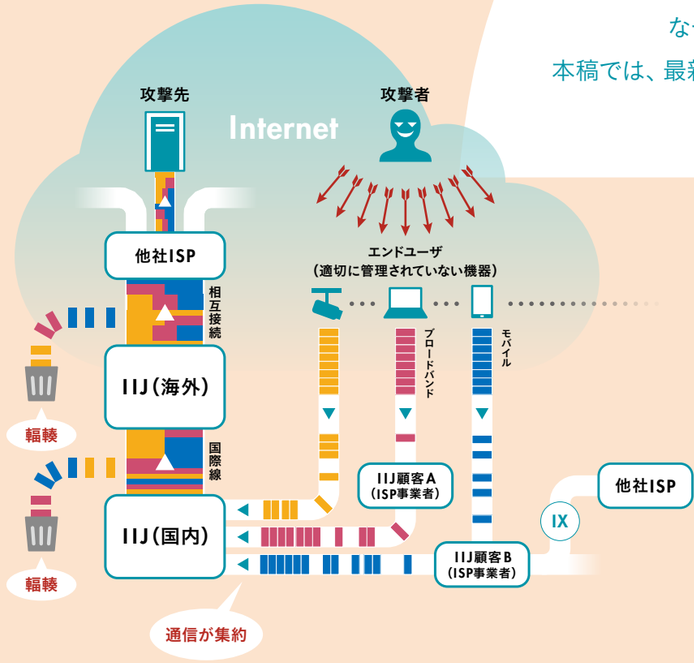
インターネットは、今や生活に欠かすことのできない社会基盤の一つになりました。安心・安全かつ安定的なインターネットの運用は、ISPのみで成り立つものではなく、法人・個人を含む全ての利用者の協力と理解が不可欠です。皆さまもその一員であるという自覚をお持ちいただき、普段からIoT機器の設定を確認するようにしましょう。

＊NAS（Network Attached Storage）：ネットワーク接続されたHDDなどの記憶装置のこと。

IoT機器を介したDDoS攻撃発生の仕組みとバックボーンへの影響

DDoS攻撃といえば、典型的なサイバーインシデントの一つだが、
最近はエンドユーザを送信元とした攻撃が急増している。
なぜ、そのようなことが起こるのか？
本稿では、最新のDDoS攻撃について解説する。

IIJ 基盤エンジニアリング本部 基盤企画部
副部長
堀 高房



IoT機器を介したDDoS攻撃

インターネット上では日々さまざまなインシデントが発生していますが、その一つにDDoS（Distributed Denial of Service）攻撃があります。「Distributed（分散）」という言葉通り、多数の送信元から大量の通信が送信先に流れ込み、WEBサーバが過負荷に陥って、正常に表示されなくなったり、ネットワークが輻輳して（飽和状態になり）正常に通信できなくなるなど、大きな影響が出ます。

DDoS攻撃と聞くと、被害を被る送信先（攻撃対象）のことを気にしがちです。たしかに、これまではIIJのバックボーンで観測されるDDoS攻撃と思しき大量通信（以下、単にDDoS攻撃と記載）は、IIJのサービスをご利用いただいているお客さまが宛先になるケースが大半でした。（それに備えるためのIIJ DDoSプロテクションサービスも提供しています）

しかし昨年夏頃から、IIJのサービス利用者であるお客さまが送信元、IIJの外部、つまりはインターネットが送信先となるDDoS攻撃が多数観測されるようになりました。その傾向は日を追って顕著になり、一一月、一二月頃にはバックボーン内で輻輳が頻発するといった実害が無視できないレベルにまで達しました。

では、なぜ送信先がIIJ内でないにもかかわらず、バックボーンに影響がおよぶのでしょうか。IIJは専用線、ブロードバンド、モバイルなどを介したインターネット接続サービスを提供していますが、それらに加えて国内の多くのISPに対してトランジットやアップストリームと呼ばれる上流回線を提供しています。送信元一つひとつの規模は小さくても、これらのISPで発生する通信が集約されてIIJに流れ込むと、最終的な規模は非常に大きくなります。実際、IIJでも数百Gbps規模のDDoS攻撃が日々観測されています。IIJのバックボーンはそれなりの規模があるので、数百Gbps程度であれば余裕を持って処理するキャパシティを有していますが、それが一箇所に集中するとなると、話は別です。

インターネットは無数のISPが相互に接続することで成り立っていますが、個々のISP同士の接続帯域には限りがあります。運悪く、あまり帯域の広くないISP間の接続を大きな通信が経由すると、その接続は簡単に輻輳します。

さらに、昨今発生しているDDoS攻撃は、送信先の多くが海外、しかも日本ではほとんど知られていないISPやサイトという特徴があります。ISPにとって上流回線はコストになりますので、通信量が多いISPとはIX（Internet eXchange）などを介して「ピアリング」と呼ばれる原則無料の相互接続を行なうことで上流回線への依存度を下げています。しかし、通信先が普段はほとんど流れない海外となると相互接続には向かず、そのまま上流回線に流れていくため、上流回線を提供するIIJのようなISPへの影響が大きくなります。また、IIJは海外にもネットワークを伸ばしていますが、日本とは高価な国際線で接続しているため、その帯域は日本国内と比較すると小さく、数百Gbpsの突発的な通信が特定の宛先向けに集中的に発生すると、どうしても輻輳しやすくなります。

なお、昨今発生しているDDoS攻撃はIIJに限った事象ではなく、規模や影響は異なるものの、多くの国内ISPで同じように発生しているようです。その全ての原因が調査されているわけではありませんが、異常な通信を発生させている機器には、7頁の「IoT機器の設定を確認しよう！」で紹介したネットワークカメラのような、いわゆるIoT機器が多数含まれていることがわかっており、それらが乗っ取られてBotnetに組み込まれ、悪意を持った攻撃者に制御されて攻撃に加担している可能性が考えられます。

エンドユーザが加害者にならないために

ひとたび通信の輻輳が発生すると、IIJのネットワークを経由する全ての通信にその影響がおよぶため、その都度、状況を確認し、場合によっては約款にもとづいて緊急の通信制限などを行なうといった対処をとります。

制限の方法はさまざまですが、DDoS攻撃の送信元は非常に多岐にわたるため、送信元を指定して制限することは現実的ではありません。そのため、致し方なく送信先のみを指定した制限となる場合もあり、その影響は異常な通信を発生させていない一般のお客さまにも波及することになります。さらに送信先もその都度異なるので、事前対処も困難です。これらは緊急対処ですが、根本的にはその送信自体を止める必要があるため、送信元となったお客さまを特定し、個別に連絡して確認と対処をお願いしています。

先に述べたようにIIJのお客さまはISPが多いので、実際の送信元となった利用者（エンドユーザ）には間接的にしか連絡をとることができず、連絡がとれたとしても、時間を要したり、なかなか対処していただけないケースもあります。また、連絡を受けたお客さまは、自分が大量の通信を発生させているという認識がなかったり、送信元がIoT機器の場合などは、その機器がインターネットに接続されていること自体に気づいていない時もあり、具体的な実例などをお話しして、身の回りの機器を確認していただくよう努めています。

このように〝無自覚な〟お客さまが送信元であっても、その影響は周りの多くの利用者を巻き込み大きく発展していき、機器を乗っ取られた被害者であると同時に（厳しい言い方になりますが……）DDoS攻撃に加担する加害者になってしまいます。

今後、5Gの普及などがさらに進めば、IoT機器の数は爆発的に増えていくでしょう。そうした状況下で適切に管理されていない機器が多数あれば、インターネットの安定性をも脅かす事態に発展しかねず、万が一そのようなことになれば、社会生活に甚大な影響をもたらすことが想像されます。

ネットワークの図を書くと、インターネットははるか彼方に存在する雲のような形で表現されますが、インターネットという特定のネットワークが存在するわけではなく、無数のネットワークの集合体がインターネットであり、利用者やインターネットを構成する機器・ネットワークもまたその一部と言えます。

インターネットにはそれを管理監督する特定の組織があるわけではなく、利用者一人ひとりが適切に使うことで成り立っている――それはある意味〝善意〟にもとづいた――自律分散のネットワークであり、安定的に使えるか否かは、利用者の行動次第なのです。皆さまにおかれましても今一度、お手元の機器の確認をお願いいたします。

Apache Log4j と Log4Shell

2021年12月、Apache Log4j の脆弱性である
Log4Shell の情報が公開された。
本稿では Log4Shell の概要と、
なぜ攻撃者が Log4Shell を悪用するのかを解説する。

IIJ セキュリティ本部 セキュリティオペレーション部
セキュリティオペレーションセンター
北山 啓思

Apache Log4j とは

Apache Log4j（以下、Log4j）は、プログラミング言語の一種であるJavaで使用されているライブラリです。おもにJava言語で開発されたソフトウェアにおいて、ログ出力機能を提供します。ソフトウェアの開発者にとってLog4jの使用は定番となっており、無償で使えることや機能の柔軟性などから、多くのJavaアプリケーションで使用されています。

例えば、Log4jがチャットアプリで使用されている場合にはメッセージの履歴を記録するために、WEBサーバで使用されている場合にはユーザからアクセスされたURLを記録するためなどに使用されています。このほかにも、アプリケーションで発生したエラーの詳細などを記録するために用いられることもあります。

Log4Shell とは

Log4Shell（CVE-2021-44228）*は、Log4jにおいてリモートから任意のコードを実行できるようにしてしまう脆弱性を指します。この脆弱性を含むLog4jを使用して開発されたソフトウェアのログに攻撃コードが出力されると、ソフトウェアが動いているコンピュータで攻撃者が意図する不正な命令が実行されてしまいます。

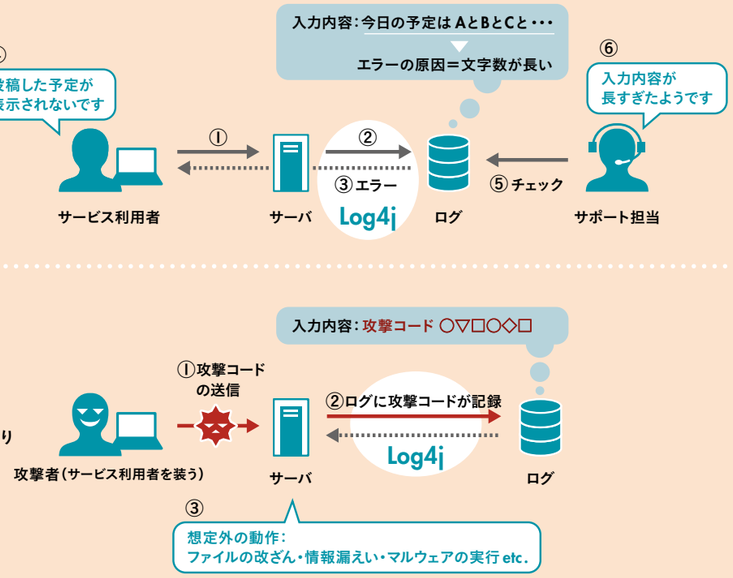
例えば、ユーザからアクセスされたURLをログに記録するWEBサーバの場合、URLに攻撃コードが含まれていると、サーバ上で不正な命令が実行される恐れがあります。不正な命令の実行に成功した攻撃者は、コンピュータに保存されたファイルの改ざんや窃取、マルウェアのダウンロードおよび実行などを試みます。

攻撃者が Log4Shell を悪用する理由

CVEでLog4Shellの情報が公開されて以降もLog4Shellを悪用する攻撃が多数観測されています。攻撃者がLog4Shellを悪用する理由としては、左記の三つが挙げられます。

- 攻撃が容易であるため。
- 攻撃の影響を受けるソフトウェアが多いため。
- 脆弱性への対策が不十分な環境が多いため。

Log4Shellにおいては、脆弱性への対策が不十分であったために攻撃されてしまう事例が確認されています。その背景には、Log4Shellが他の脆弱性と比較して、影響範囲の特定が困難であることが挙げられます。ソフトウェアの使用にあたり、ユーザがライブラリを意識することはあまりないため、どのソフトウェアでLog4jが使用されているかが明らかではありません。またLog4jは多くのソフトウェアで使用されているため、システム管理者が意識していない箇所で使用されていることもあります。これらの要因から、Log4Shellへの対策が不十分な環境が残っており、攻撃者はLog4Shellの悪用を試み続けているのです。



今後の対応

Log4Shellは、影響範囲の特定が困難であると説明しました。そのため、組織内で対策がされていないソフトウェアがまだあるかもしれません。Log4Shellをはじめ、今後、同様の脆弱性が公開された際、被害を最小限にするためにも、改めて組織内で使用されているソフトウェアを確認することをお勧めします。おもな確認事項は、左記の三点です。

- ソフトウェアの一覧。
- ソフトウェアのバージョン。
- ソフトウェアの開発元・連絡先。

特にインターネット上で公開されているサーバで動作するソフトウェアの情報は、必ず把握しておきましょう。脆弱性が公開されたら、早急に影響の有無を確認できる状態にしましょう。また、サーバへの攻撃は、**IDS／IPS**や**WAF**で遮断・検知できる場合があります。ソフトウェアの早急なアップデートが困難な場合は、これらのセキュリティデバイスの利用もご検討ください。

そのほかにも、社内のみで使用されるソフトウェアや社員の端末で使用されるソフトウェアが攻撃の対象となる可能性もあります。特にWEBブラウザ、メールクライアント、チャットアプリのようにインターネット上から得られる情報を処理するようなソフトウェアは、攻撃の対象となる危険性があります。社員が使用するWEBブラウザなどに脆弱性の影響がおよぶ場合には、メールなどで注意喚起できる状態にしましょう。

IIJにできること

ここでは、世界中に影響をもたらしているLog4jというライブラリの脆弱性について解説しましたが、影響の大小にかかわらず、セキュリティインシデントは日々発生しています。

IIJの**SOC**（セキュリティオペレーションセンター）では、二四時間三六五日、お客さま環境下で発生するセキュリティインシデントの対応にあたっています。SOCで観測したセキュリティインシデントの情報は、月に一度、「wizSafe Security Signal」としてWEBで公開しています（https://wizsafe.iij.ad.jp/）。こうした活動が皆さまの今後のセキュリティ対策の一助になれば幸いです。

＊2021年12月9日、Apache Software Foundationは、同社の提供するApache Log4j 2の複数バージョンにリモートコード実行の脆弱性（CVE-2021-44228）が存在することを公表した。https://logging.apache.org/log4j/2.x/security.html#log4j-2.15.0

おさえておきたい セキュリティ・キーワード

本特集に出てきたセキュリティ用語をわかりやすく解説します！

1. なりすましメール

無関係の送信者が特定の企業や人物を装い送信してくるメールで、差出人のメールアドレスや関連情報、件名や本文が本物であるかのような内容となっており、受け取った相手を本物と信じ込ませようとします。

なりすましメールにはいくつか種類がありますが、その目的には、金融機関やオンラインサービスを装い、偽のログイン画面に誘導することで、認証のための情報（ID やパスワード）、カード番号などを盗み出すフィッシング詐欺があります。

また、添付ファイルを開いたり、本文などにあるリンク先をクリックすることで、不正プログラム（マルウェア）に感染させる場合もあります。マルウェア感染の目的は、内部の機密情報を抜き取ったり、ファイルを暗号化することで利用できないようにしたうえで、金銭を要求することです。このような身代金を要求するマルウェアは特にランサムウェアと呼ばれます。なりすましメールは、こうした犯罪行為の最初の手段として用いられます。

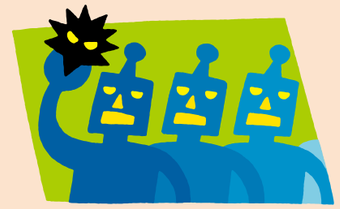
2. DDoS (Distributed Denial of Service) 攻撃

日本語に訳すと「分散型サービス拒否攻撃」。インターネットを介した攻撃手法の一つで、悪意のある攻撃者がターゲットとなるホスト（コンピュータやネットワーク）に対して複数箇所より大量の攻撃パケットを送り込み、標的を機能停止状態にする攻撃のことです。

IIJ では、「IIJ DDoS プロテクションサービス」を提供しており、平常時の通信状態を逸脱した異常な通信を自動検知し、攻撃パケットを遮断するなど処置をとることで、お客さまのサーバやネットワークを保護し、インターネットへの接続回線も守ります。

3. Botnet

Bot はロボットの略語で、人の作業を代行したり、人間のように振る舞うソフトウェアやシステムのことです。悪意のあるソフトウェアのなかにもボットと呼ばれるプログラムがあり、攻撃者の指示で遠隔から指令された動作を行ないます。そして、インターネット上で同じボットが組み込まれたシステムネットワークのことを「Botnet（ボットネット）」と呼び、攻撃者の指示でいっせいに特定のネットワークへ DDoS 攻撃を行なったり、迷惑メールの発信元として悪用されます。



4. CVE (Common Vulnerabilities and Exposures)

情報セキュリティにおける脆弱性やインシデントに固有の名前や番号を付与し、リスト化した事典です。CVE が登場するまでは、各種製品ベンダやセキュリティベンダが、脆弱性に対して独自に名前を付けていたため、ベンダが公表する脆弱性情報はばらばらで、ある脆弱性情報が同じ問題についてのものなのか、判別することは困難でした。また、脆弱性のデータベースや対応ツールの互換性も有効性に乏しいものになっていました。

そうした状況を改善するため、米国政府の支援を受けた非営利団体の Mitre Corporation（マイター・コーポレーション）が 1999年、脆弱性を一意に特定できるよう「CVE」を提案・実装しました。CVE の登場で脆弱性の一つひとつに固有の名称と CVE ID と呼ばれる固有の番号が付与され、脆弱性情報の共有・比較が容易になりました。

現在では、主要なベンダなどから脆弱性情報が公開されると、必ずと言っていいほど CVE と CVE ID が付与されたうえで公開されています。これまでに付与された CVE と CVE ID の一覧は、Mitre Corporation の WEB サイト（http://cve.mitre.org/cve/）で閲覧できます。

※出典：https://www.nic.ad.jp/ja/basics/terms/cve.html

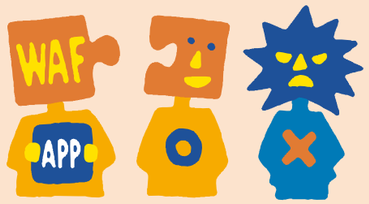
5. IDS (Intrusion Detection System：不正侵入検知システム) IPS (Intrusion Prevention System：不正侵入防止システム)

IDS は、ネットワーク型 IDS とホスト型 IDS があり、ネットワーク型 IDS は、ネットワークに流れるトラフィックを監視して、不正アクセスや異常通信を検知した際に管理者に通知します。サーバ型 IDS は、サーバ上でトラフィックやプロセスなどを監視して、同様に管理者に通知します。IPS はネットワーク型 IDS の機能に加えて、検知した不正アクセスや異常通信を遮断できます。

従来のファイアウォールやルータは、IP アドレス、ポート、プロトコル（TCP／UDP）レベルでパケットをフィルタリングするため、これらが許可されている通信の不正アクセスや異常通信を防ぐことはできません。そこで、IPS や IDS がファイアウォールを補完するかたちで導入されます。IIJ では、マネージド型の IPS／IDS サービスを提供しており、最新のインターネットの脅威に対して IIJ 独自のシグネチャを作成し、それらの攻撃に迅速に対応し、お客さまのサーバやネットワーク環境を守ります。

6. WAF (Web Application Firewall)

WEB サイト上のアプリケーションに特化したファイアウォールで、HTTP、HTTPS 通信を監視して、WEB アプリケーションの脆弱性を突く攻撃から WEB サイトを守る役割を果たします。IIJ では、マネージド型の WAF サービスを提供しており、SQL インジェクションやクロスサイトスクリプティングに代表される WEB アプリケーションの脆弱性から、お客さまの WEB サーバを保護します。



7. SOC (Security Operation Center)

セキュリティ機器やネットワーク機器から得られるログを 24 時間 365 日、監視・分析し、脅威となる事象の発見・特定・通知を行なう組織です。ひと昔前は、サイバー攻撃はおもに企業が管理するサーバを対象としていましたが、近年は社員が利用する PC、タブレット、スマートフォンなどの端末にまで広がり、守るべき範囲が拡大する一方、攻撃手法も高度化・複雑化しており、従来のセキュリティ機器による対策だけでは防御しづらくなっています。こうした背景から、ますます SOC の重要性が高まっています。

IIJ の SOC では、独自のセキュリティインテリジェンス（ISP として保持するバックボーントラフィックや DNS 情報、お客さまに提供しているファイアウォール、メール、WEB サイトといった各種サービスの膨大なログ・イベント情報を自社で構築した情報分析基盤へ集約し、ビッグデータ解析して生成）を活用し、発見が困難な脅威にも対応しています。SOC の設備は、攻撃検知・通知・対処を行なう「オペレーションルーム」と、未知のマルウェア解析やフォレンジック調査など、セキュリティリスクの高い情報を扱う「セキュリティラボ」から構成されています。IIJ が提供する SOC サービスは、セキュリティログの収集・分析からインシデント対応まで、専任チームがお客さまに代わってセキュリティ脅威を監視し、迅速に対応します。

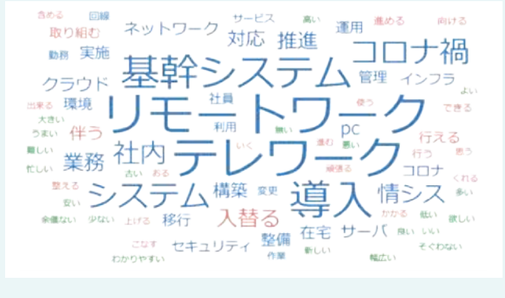
IIJ Research
となりの情シス

アンケート
2021年、情シスの皆さんの「頑張ったこと」

IIJ では、情報システム部門（以下、情シス）の頑張りを広く紹介するために「情シス頑張ったことアンケート 2021」と題した調査を実施しました。今回はその集計結果をダイジェスト版でお届けします。

（実施期間：2021年12月3日～12月27日／有効回答数：569件）

Q1. 情シスとして「これは頑張った！」と思える2021年の取り組み・活動は？



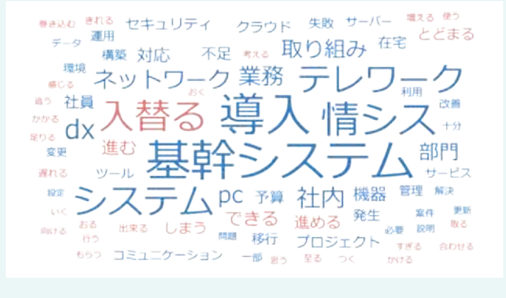
参考：前回（2020年）の結果

※「ユーザーローカル テキストマイニングツール」による分析

「頑張った取り組み」のなかでリモートワーク、テレワーク関連のコメントを拾っていくと、導入済みの環境の強化・改善などが多く見受けられました。

- 通信インフラの高速化、オフィスのフリーデスク化、社内ポータルのクラウド化、リモートワーク接続方式の変更（リモートデスクトップ方式⇒リモートアクセス方式）、勤怠管理システムのバージョンアップ。
- コロナ禍で始まったリモートワークやWEB会議・WEBセミナーなど、従来はさほど重要視されていなかったインターネット環境・モバイル環境であったが、日常の業務スタイルが大きく変わり、必要不可欠なシステムとしてクローズアップされたと同時に、安定的に利用できることが重視され、これに応えるべく新たな環境への導入や社内業務へのスムーズな展開、日々のサポートなど試行錯誤を繰り返しながら改善を図った。

Q2. 「ここは失敗した、惜しかった」と感じた2021年の取り組み・活動は？



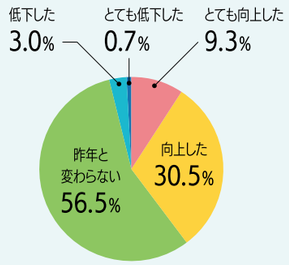
参考：前回（2020年）の結果

※「ユーザーローカル テキストマイニングツール」による分析

失敗した取り組みとしては「基幹システム」、「DX関連」における計画の遅延や中断といったコメントが多く寄せられました。

- DX化を進めていたが、経営層とのコミュニケーションが少なく、最後の最後で中止になってしまった案件があった。
- DX化の初期段階として「アナログからデジタル」へ、など全社に向けて推進してきたが、全国の拠点への説明不足もあり、地域によって格差が生じてしまった（東高西低）。
- 一部の基幹システムをクラウドに移行したが、投資効果が適正に把握できていない。
- 半導体不足により、思うように基幹システムの入れ替えができないこと。
- 基幹システム再構築においてコロナ禍の影響をもろに受け、業者の開発が大幅に遅れ、開発予定人員が減り、品質も低下した。

Q3. 昨年に比べ、社内での情報システム部門の存在感は向上した、と感じますか？



約40％が「存在感が向上した」、約57％が「変わらない」と回答しました。存在感を向上させた具体的な取り組みを聞いたところ、「組織・戦略・コスト削減施策」といった意見が目立ちました。

- 全社的にDX化に取り組み、現場との意見交換などを積極的に行なって、「顔の見える」情報システム部門になれた。
- 全社員から既存システムの改善要望を出してもらい、改善計画を作成したり、在宅勤務がいつでも可能になるようHWの整備と仕組みの導入などを行なった。
- ①複数名の社長やマネージメントを委員とした「IT戦略委員会」の発足・運営・推進。②工事現場業務へのタブレット型モバイルツールの活用提案とトライアル実施。③同現場へのウェアラブルカメラ、リモートコミュニケーションツールの活用提案とトライアル実施。④プロジェクト文書管理パッケージツールの紹介・導入・運用開始。
- チャットボットの導入による問い合わせへの24時間対応の実施。各種アップデートの遠隔化によるユーザの負担軽減。

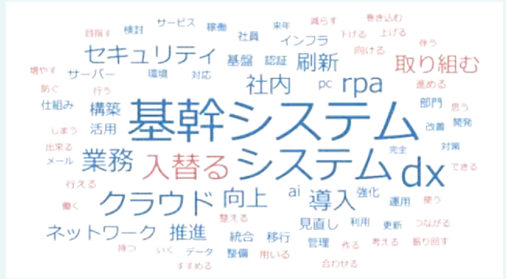
Q4. 情報システム部門の2021年を漢字1文字で表すと？

1位	忍	（56票）	やるべきことはやらないといけないが、会社の理解を得るのに時間がかかった。それを我慢しながらの業務遂行であった。 不平・不満、一部批判めいたものも聞こえてくる・寄せられるなか、耐えて頑張ってます。
2位	忙	（36票）	忙しいにつきる。これ以上の言葉は浮かばない。
3位	耐	（34票）	他部署のITに関する無理解からくる無茶な要望、特別に頑張って対応したケースを当たり前にされてしまうなど、社内の扱いに耐えたため。
4位	変	（22票）	コロナ禍ということで、仕事のやり方や中身が変化している。それを支えていく、導くのは情シスだと思う。
5位	進	（14票）	とにかく、前に進む、チャレンジする。チャレンジしながら方向修正し、ダメなら撤退する。

6位以下 疲（12票） 遅・難（9票） 改・苦（8票） 転・楽（5票）

「忍」、「忙」、「耐」という漢字が上位にランクインし、コロナ禍対応やDX推進など、働き方やオフィス環境に変革が求められるなか、情シスが裏方として迅速かつ忍耐強く活動していたことがわかりました。

Q5. 今年2022年、新たに取り組みたいことは？



参考：前回（2020年）の結果

※「ユーザーローカル テキストマイニングツール」による分析

基幹システム関連ではシステムの刷新やリプレース、DX・デジタル化関連ではDX推進や具現化などに関するコメントが多く寄せられました。

- デジタル化による現場の改善促進と、DXによる従来業務の枠を越えた取り組みを開始したい。
- ペーパーレス化やDXを進め、社内スタッフの業務を楽にしたい。
- 構内LAN、社内WAN、インターネット接続など、ネットワークの稼働状況を分析し、基幹システムの更新（クラウド化）に合わせて、最適なネットワーク環境を企画・構築する。
- 基幹システムAPIの設計、重要機能のWEB化を進められれば、来年はもっといいことができると期待しています！
- 前年からの継続作業である基幹システムの更新作業、ITベンダとの折衝、現行システムの仕様の取りまとめと新しい機能要望の取りまとめ。
- 全社における基幹システムのリプレース検討。

今回は「情シス頑張ったことアンケート2021」の集計結果の一部を紹介しました。これら以外にも、誌面では紹介しきれなかった調査項目がありますので、特設サイト「法人IT調査レポート」も、ぜひご覧ください。
特設サイトでは、今回ご紹介したレポートのほかにも、情報システム部門に関するさまざまな調査結果を紹介しています。
日頃の業務にお役立ていただければ幸いです。　特設サイト「法人IT調査レポート」 https://www.iij.ad.jp/svcsol/survey/

人と空気とインターネット

新たな価値を創造するIT活用

――非常勤顧問
浅羽 登志也

既存のサービスをIT化するのなら、新たな価値（体験）を創出してほしい――今回は、そう考える筆者が最近、興味を惹かれた二つの事例を紹介する。

シャドウワークからは何も生まれない

ついに拙宅の近所のスーパーにも自動レジが設置されてしまいました。商品のバーコードを読み取らせ、袋に詰め、精算方法を選び、カード決済をする。何度かやればすぐできるようになりますし、なんとなく楽しくはあるのですが、でも、ふと自動レジの横に目をやると、そこには有人レジがずらりと並び、オペレータの皆さんが、いつやってくるかわからないお客を（大変失礼な言い方ですが、暇そうに……）待っています。混雑している時間帯なら、有人レジももっと稼働しているのでしょうが、しばらくは並行運用をして、それぞれの稼働率などのデータを集めて、きっと有人レジが減らされるのだろうなぁと思うと、とても寂しい気分になります。だからと言って、あえて有人レジを使うのもなんだかなぁと思いつつ、自動レジでピコピコとバーコードを読み取らせるというアンビバレンツな気分で買い物体験をしています。

どうせIT化で人が削減されるのであれば、もっと凄いこと、少なくとも何か新しいことができるようになって欲しいものです。現状の自動レジは、以前も登場したイヴァン・イリイチ先生のおっしゃる「シャドウワーク」に過ぎません。シャドウワークの定義はいくつかあるのですが、ここでは「消費社会を回すうえで、消費者側が無償でさせられる労働（費用計上されない労働＝シャドウワーク）」としましょう。言い換えると、販売側のコスト削減のために、消費者に転嫁される無賃労働です。

少し考えればおわかりいただけるように、このようなIT化からはいくら続けても新たな価値など何も生まれませんし、ただ我々の労働が搾取されるだけです。こんなIT化ばかり続けていくと、日本人はどんどん貧しくなる一方です。では、新たな価値を創造するIT活用とは、どのようなものでしょうか？

オンラインで注文するオリジナル・コーヒー

109シネマズ川崎と二子玉川の二箇所に、サントリーが運営する「TAG COFFEE STAN(D)」というコーヒーサービスが昨秋オープンしました。これはスマホやタブレットでWEBにアクセスし、自分用にコーヒーをカスタマイズできるサービスで、ベースドリンク（ブラック／ラテ）濃さ（オリジナル／ライト）、甘さやフレーバーなどを選択肢のなかから選べて、さらにボトルのラベルに二〇〇〇種類以上のバナーデザイン（なかには上映中の映画とコラボしたものもある）を選び、そこに名前やメッセージなどのテキストを自由に掲載できるというものです。

オンラインで注文して、店舗でバーコードを見せて受け取りと決済を行ないます。その日の気分や観る映画に合わせて味わいやラベルを特別なものにしつらえて映画を鑑賞するという、ちょっと新しい体験ができるわけです。お客がWEBでカスタマイズするのは「シャドウワーク」的とも言えますが、その見返りにオリジナルのラベル付きで、味もカスタマイズされた自分専用のコーヒーが得られるのですから、ITによってこれまでになかった新たな体験価値が提供されていると言えそうです。

興味深いのは、かつて東京・日本橋にTOUCH-AND-GO COFFEEという名前で、この店舗の実証実験店舗があったことです。こちらはLINEでコーヒーの味やラベルをカスタマイズして発注・決済し、指定時間に店舗に行けば、専用ロッカーに入れられた自分用のコーヒーを受け取れるというサービスでした。忙しいビジネスパーソンが時間をかけずに好みのコーヒーを得ることを目指したものだったそうです。この店舗は、二年間の実験を終えて二〇二一年夏に閉店したのですが、その間に得られたデータをもとに、正式店舗向けにサービス内容が変更されたそうです。一つは選べるコーヒーのオプションが減ったこと、もう一つはカスタムラベルのバナーの種類や入力可能文字数が大幅に増加したことです。もともとカスタムラベルの文字は自分の名前を入れることを想定していたそうですが、実験の結果、プレゼント用に友達の名前を入れたり、お気に入りのキャラクターやアイドルの名前を入れる人のほうが多いことが判明。コーヒーのカスタマイズのほうがニーズが高かったわけです。そこでターゲットをビジネスパーソンから、エンタメ施設をおもに利用する女性へと方向転換し、立地や内容もそれに合わせて変更したというのです。このようにβサービスから集まったデータをもとに内容をアップデートするやり方は、まさにITを活用した価値創造のサイクルを踏まえたサービス開発と言えます。

アバターロボットが働くカフェ

さらに仰天のサービスを提供する店舗を最近見つけました。日本橋にある「分身ロボットカフェDAWN ver.β」です。なぜ日本橋にそういう店舗が集まるのかは不明ですが、そこではなんと、ウェイトレスのような外見をしたロボットが接客を行ない、コーヒーや食事を席に運び、お客と談笑したりしているのです。さらに、店の奥では少し大きめのバリスタロボットがお客の注文に応じてカスタムコーヒーを淹れているではありませんか。

実はこれらのロボットは「パイロット」と呼ばれる、重度の障害や病気で外出できない人たちが、ネット経由で遠隔操作しているというからさらに驚きです。つまり、ロボットを「アバター」として活用し、障害や病気を持つ人に働く場を提供しているのです。席で私の注文を受けてくれたのは、岡山市に住む方、コーヒーを運んで来たのは奈良県の方、実験サービスと言ってフローズンアイスを席まで売り込みに来たのは小平市の方……等々。外見は皆同じアバターロボットでも、少し会話をすれば個性も伝わり、楽しくお話しさせていただきました。これはまさにICTを活用したロケーションフリーな新たな働き方の創造と言えるでしょう。

店を運営しているのはアバターロボットを開発した株式会社オリィ研究所というベンチャー企業です。彼らはテクノロジーによって、人々の新しい社会参加のかたちを実現するという理念を掲げて活動しています。この店舗は、少し先の未来を体験してもらうための実験店舗という位置付けだそうです。アバターロボットを活用する取り組みは、障害者だけでなく、今後増加する高齢者の働く場の提供や、それとは逆に遠隔からの高齢者見守り・サポート、さらには新たなパンデミック下での社会活動の維持など、さまざまな可能性を感じました。

ただし、アバターロボットの動作はまだまだぎこちないというのが正直なところ。「今日は調子が悪いんですぅ」と言いながら店員さんが、なかなかうまく前進できないアバターを押したり、向きを変えたり、サポートしながらの運営。まさにβサービスの状態でした。

もう一つ面白いのは、お店がくれた会員証に「見習い研究員」と書かれている、つまり、お客を実験に参加する研究員に見立てている点です。それでお金を取るとはけしからん！　これこそシャドウワーク、いや、お金を払っているので、それ以下だ！　と言う人がいるかもしれません。でも私は、むしろ開発者と一緒に新たな価値創造のプロセスに参加しているようで少しワクワクしました。デジタルとリアルサービスの融合による新しい価値は、このような提供者と利用者の共創から生まれるのではないでしょうか。カフェを離れたあとも、今まで使っていなかった脳の部位が活性化されたようで、あれを活用するにはどうすればいいか、常に考えているような感じです。βサービス後の正式サービスがどのようなかたちになるのか、とても楽しみです。

このカフェ、三回行くと主任研究員に昇格できるそうなので、また機会を見つけて行ってみようと思います。

イラスト／末房志野

新企画

社会を支えるIIJ

インターネットと作る未来
「災害時の情報連携」編

IIJ が提供するサービス・ソリューションで、
地域社会の暮らしや未来を支える取り組みを紹介します。

茨城県常総市は、平成27年9月関東・東北豪雨にともなう
鬼怒川の大規模氾濫に見舞われた際の教訓を活かし、
災害時の要援護者情報を共有するシステムとして
「IIJ電子＠連絡帳」を導入しました。

2021年、常総市で災害対策訓練が実施されました（写真左）。その際、疑似的な情報とIIJ電子＠連絡帳を使い、地域の専門職が要援護者の安否情報などを地図上に登録して、多職種間で共有を図る訓練も行なわれました（写真上）。

（写真提供：常総市）

関東・東北豪雨で浮かび上がった課題

平成 27 年 9 月関東・東北豪雨による鬼怒川の大規模氾濫に見舞われた茨城県常総市では、市役所の職員、ケアマネージャーなどが、要援護者[*1]の安否確認や安全確保に奔走することになりました。市役所の庁舎が水没して要援護者の居所や安否情報が把握できなくなり、薬の処方に不可欠な電子カルテの情報も参照できなくなりました。現場では、リアルタイムな情報共有や災害を想定したデータの保護など、さまざまな課題が浮き彫りになりました。

セキュアな環境でデータを守る

「医療や介護の情報は、災害に耐え得る安全な場所に保管し、セキュリティを確保しなければ、地域を持続的に守っていけない」。常総市と、きぬ医師会は、IIJ電子＠連絡帳を平時の医療介護連携と災害時の情報連携に応用する方針を決めました。通常時、IIJ電子＠連絡帳では、在宅療養者の支援に携わる専門職間でのみ情報共有を行ないますが、災害時には防災・救急・行政の関係者が一体となって、避難行動の支援を行なう必要があります。IIJ電子＠連絡帳は有事の際、地域の関係者が要援護者の安否情報と支援状況を共有する仕組みを持っています。

まとめ

もともと医療介護連携のためにスタートしたIIJ電子＠連絡帳は、複数分野の専門職[*2]が集まるソーシャルネットワークとなりつつあります。IIJは、IIJ電子＠連絡帳が地域社会のプラットフォームとなり、防災・救急・医療・介護などの地域課題を解決し、住民が幸せに暮らせる世界を作っていけたらと考えています。

＊1 要援護者：災害時に自力での避難行動や避難所などでの生活が困難なため、行政の支援が必要な高齢者や障害者の方々。

＊2 専門職：医師、訪問看護師、ケアマネージャー、ヘルパー、薬剤師など、要支援者の生活を専門家の立場からケアする人。

もっと詳しく

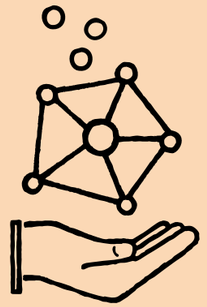
動画・インタビュー記事では、常総市役所の皆さまや地域の医師のインタビューを通じて、IIJ電子＠連絡帳の導入経緯や成果を紹介しています。

動画　　インタビュー記事

Internet Trivia

インターネット・トリビア

データセンターのサーバの変遷



IIJ MVNO事業部 事業統括部
シニアエンジニア
堂前 清隆

データセンターというと、多数のコンピュータが搭載されたラックが整然と並んでいる様子を思い浮かべる方が多いのではないでしょうか。今回は、データセンターとそこに設置されるコンピュータ（サーバ）の変化を振り返ります。

実は、インターネットが普及し始めた1990年代前半、今のようにデータセンターに多くのサーバは置かれていませんでした。データセンターという名前も一般的ではなく、ネットワークセンターや通信局舎と呼ばれ、設置されている機器もおもに通信機器でした。お客さまの社屋から引き込まれた通信回線を接続するルータなどに混じって、サーバが置かれているといった具合です。今ではサーバを設置するためのラックのように見える「19インチラック」も、もともとは通信機器を設置するのが主目的でした。

この時代、インターネットで利用するような小型～中型のサーバは、19インチラックに固定できるものがあまり出回っておらず、卓上に置くUNIXワークステーションをベルトでくくりつけたり、パソコン用の汎用部品を組み込むラックマウント用のケースなどが使われていました。

2000年頃に登場した「1Uサーバ」がこの状況を変えました。1Uサーバは、サーバメーカがラックマウントを前提として部品から筐体まで設計したものです。これにより、ラックマウント機器の規格である1U（高さ約44.5ミリ）に一台のサーバが納められるようになり、従来に比べて3～4倍の密度でサーバを設置できるようになりました。

ただ、1Uサーバも良いことばかりではありませんでした。高さを1Uに抑えるためにCPUなどを冷却するファンのサイズが制限され、それが原因で激しい騒音が発生するなど、小型化にはデメリットもあったのです。

そんな困難がありながらも、さらなる高密度化が図られました。2002年頃に登場したブレードサーバは「刃（ブレード）」のような細長い板にサーバの主要部品を搭載し、このブレードを外枠になる「エンクロージャ」に多数取り付けることで密度を高めました。メーカによって規格は異なりますが、例えば3Uサイズでサーバ18台分のブレードを搭載するといった感じで、かなりの高密度が達成できました。

ただ、ブレードサーバは高密度化を進めすぎたのかもしれません。もともと通信機器が主体だったデータセンターに、大量の電力を消費するサーバを高密度に設置した結果、供給電力の限界を超え、さらには空調システムの限界も超えて冷却が追いつかなくなるという事態が発生したのです。結局、ブレードサーバは数年で廃れ、1Uやその倍の2Uサイズのサーバが業界標準として使われるようになりました。

その一方で、新しい試みもあります。先に書いたとおり、冷却の問題などで19インチ・1Uサイズというのは必ずしもサーバに適したサイズではありません。多くの通信機器が19インチラックに設置されていたため、それにサーバも合わせた結果でした。

クラウド時代が訪れ、データセンターに置かれる機器の主役がサーバになってくると、サーバに適した規格を新たに作ろうという動きが起りました。そうしたチャレンジの一つが、2011年にFacebookによって提唱され、その後150社以上が参加することになった「Open Compute Project（OCP）」です。OCPはサーバだけでなく、ラックについても新しいデザインガイドを提案しました。あくまでOCPは大規模なインフラのための規格なので、すべてのサーバがOCPに置き換わるわけではありませんが、データセンターのなかではこういう変化も起っているのです。

イラスト／末房志野（P20,21）

Global Trends

グローバル・トレンド

シン・グローバルを目指すSafous

IIJグローバル事業本部
グローバル事業推進部
田中 三貴

先行者となり、状況を変えたい

二〇二一年一一月、IIJはゼロトラストの技術をベースとしたリモートアクセスサービス「Safous」（セーファス）をリリースしました。「利用者の快適さとネットワークの安全性を、手間をかけずに確保したい」。Safousは、こうした情シス部門の願いを叶えるサービスです。Safousは今後、WEBアクセスのセキュリティ機能やクラウドの利用状況を可視化する機能などを追加し、統合的なセキュリティ対策サービスとして開発を進めていきます。

ジャカルタ、シンガポールといった大都市に営業拠点こそ設けていますが、IIJの海外向けサービスは、日本国内で企画・開発したサービスを海外向けに応用するものが大半でした。残念ながらIIJ自身、同地ではメジャーとは言い難い存在です。この状況を変えるのがSafousです。Safousは最初から、環太平洋での販売を目標に定めて企画・開発しました。

米国や欧州に比べると、アジアはITの利活用において遅れをとっています。ゼロトラストという概念も、それを取り入れたサービスも、まだほとんど認知されていません。そこで今回、我々はニーズが顕在化する前に、ゼロトラストを「IIJから」アジアの方々に知ってもらい、「IIJから」サービスを利用する環境を作ろうとしています。

チャネルセールスとデジタルマーケティング

その狙いを達成する手段は、二つあると考えています。一つは「チャネルセールス」です。現在、各エリアの現地法人がSafousを売る販売代理店網を作り始めています。もう一つは、物理的な距離を超えることができる「デジタルマーケティング」です。環太平洋地域のなかでもまずはASEANを中心に展開していきますが、大きなチャレンジとしてオーストラリアでも、デジタルマーケティングを推進していきたいと考えています。営業拠点はありませんが、英語が公用語で、それなりの市場規模があり、時差がないオーストラリアでマーケティングが成功すれば、他地域に展開する際のよいベンチマークになります。もちろん、どちらの手段においても、先行者たるには〝スピード感〟が欠かせません。

Safousは、これからのIIJのグローバル戦略の最初の一歩でしかありません。我々はチャネルセールスとデジタルマーケティングを販売手法の主軸に据え、欧米にも市場を広げていきたいのです。商材となるのはSafous同様、最初からグローバル市場での展開を目指して開発したサービスです。Safousで培われたノウハウや販路は、今後のサービス開発に役立つはずです。

株式会社 インターネットイニシアティブ

本社　東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-4466

関西支社　大阪府大阪市中央区北浜 4-7-28 住友ビルディング第二号館 5F
〒541-0041　TEL:06-7638-1400

名古屋支社　愛知県名古屋市中村区名駅南 1-24-30 名古屋三井ビルディング本館 4F
〒450-0003　TEL:052-589-5011

九州支社　福岡県福岡市博多区冷泉町 2-1 博多祇園 M-SQUARE
〒812-0039　TEL:092-263-8080

札幌支店　北海道札幌市中央区北四条西 4-1 伊藤・加藤ビル 5 階
〒060-0004　TEL:011-218-3311

東北支店　宮城県仙台市青葉区花京院 1-1-20 花京院スクエアビル15F
〒980-0013　TEL:022-216-5650

横浜支店　神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-470-3461

北信越支店　富山県富山市牛島新町 5-5 タワー 111 10F
〒930-0856　TEL:076-443-2605

中四国支店　広島県広島市中区銀山町 3-1 ひろしまハイビル 21 5F
〒730-0022　TEL:082-543-6581

沖縄支店　沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル
〒900-0015　TEL:098-941-0033

新潟営業所　新潟県新潟市中央区南笹口 1-1-54 日生南笹口ビル 7F
〒950-0912　TEL:025-244-8060

豊田営業所　愛知県豊田市西町 4-25-13 フジカケ鐵鋼ビル 5F
〒471-0025　TEL:0565-36-4985

IIJグループ／連結子会社

株式会社 IIJエンジニアリング
東京都千代田区神田須田町 1-23-1 住友不動産神田ビル 2 号館 15F
〒101-0041　TEL:03-5205-4000

株式会社 IIJグローバルソリューションズ
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-6777-5700

株式会社 IIJプロテック
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6766

株式会社トラストネットワークス
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6490

ネットチャート株式会社
神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-476-1411

IIJ America Inc.
55 East 59th Street, Suite 18C, New York, NY 10022, USA
TEL：+1-212-440-8080

IIJ Europe Limited
1st Floor 80 Cheapside London EC2V 6EE, U.K.
TEL：+44-0-20-7072-2700

PTC SYSTEM (S) PTE LTD
Jackson Design Hub 29 Tai Seng Street #04-01 Singapore
TEL：+65-6282-0255

発行／株式会社インターネットイニシアティブ 広報部
お問い合わせ／株式会社インターネットイニシアティブ 広報部内「IIJ.news」編集室
〒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
TEL: 03-5205-6310　E-mail: iijnews-info@iij.ad.jp

編集／村田茉莉、鈴木健二、小河文乃
編集協力／合同会社 Passacaglia
表紙イラスト／末房志野
デザイン／榊原健祐、榊原吏海（Iroha Design）
印刷／株式会社興陽館 印刷事業部

表紙の言葉「花道」

春は出会いと別れの季節とも言われます。去り行く別れを見送ることもあれば、新しい出会いを迎えることもあります。惜しまれながら見送られる人、「ようこそ」と喜んで迎えられる人は、まるで花道を歩く主役のようです。新生活の始まりや人の移動・異動など、活力に満ちた華やかな季節です。

末房志野

◎IIJ.news表紙のデザインを壁紙としてダウンロードいただけます。ぜひご利用ください。
URL: https://www.iij.ad.jp/news/iijnews/wp/
◎IIJ.newsのバックナンバーをご覧いただけます。URL: https://www.iij.ad.jp/iijnews/

編集後記

花粉症のため、この時期は何度もくしゃみをするし、目がかゆくなります。それもあってか、コンタクトレンズをすると目に痛みが走るようになりました。そこで、眼鏡に変更して過ごしていたところ、もう戻す必要もないかという考えになり、長年コンタクトレンズ派でしたが、この 3 月で卒業することにいたしました。残りの使い捨てコンタクトレンズには申し訳ないですが、春はお別れのシーズンということで処分することにします。(K) ／友人 4 人と 1 泊 2 日で伊東に出かけました。家族以外で旅行するのは出産以来なんと 10 年ぶり！ 旅行を計画してから当日を迎えるまで日に日に楽しみが膨らみ、当日、東京駅のホームで待ち合わせて観光特急列車「列車サフィール踊り子」（しかも個室！）に乗り込むころには興奮のあまりドキドキがとまらず、このまま楽しい時間が 1 日続くと思うと、旅の途中で心臓が止まるのではないかと心配になるほどでした。女 5 人、ひたすらしゃべり続け、温泉につかってお酒を飲み、さらにしゃべり続ける――10 年ぶりの友人との旅行は言うまでもなく最高の時間でした。(M) ／本号の表紙を見た瞬間「季節を選ぶ柄だけど、これは名古屋帯にしたい！ 三分紐は空と同じ水色で、帯留めは貝製のモンシロチョウ。着物は生成に近い白の、ごく控えめな江戸小紋で…」などとウキウキしてしまいました。本社オフィス界隈では、和服の人が行き来する姿をときどき見かけます。自分は着物を着る習慣がなくても、そんなことをつい考えるのは春の麗らかな気候のせいかもしれません。(A)

Information

1 セキュリティ専門ポッドキャスト番組「セキュリティのアレ」が「サイバーセキュリティに関する総務大臣奨励賞」を受賞

IIJセキュリティ本部セキュリティ情報統括室長の根岸征史がパーソナリティの一人として運営に参加するセキュリティ専門ポッドキャスト番組「セキュリティのアレ」が、2021年度「サイバーセキュリティに関する総務大臣奨励賞」を受賞しました。同賞は、総務省がサイバーセキュリティ対応の現場において優れた功績をあげている個人・団体を表彰するものです。

「セキュリティのアレ」は、日本初のセキュリティ専門ポッドキャスト番組として2011年2月にスタートし、継続的に毎月数本の番組を配信しています。SBテクノロジー株式会社の辻伸弘氏、セキュリティリサーチャーの piyokango（ピヨカンゴ）氏、IIJの根岸征史の3名がパーソナリティを務め、各々が専門的立場から、セキュリティインシデントや攻撃手法に関する最新情報、セキュリティ関連の時事情報、新しいセキュリティ技術などをわかりやすく紹介しています。

詳細（IIJ プレスリリース）
https://www.iij.ad.jp/news/pressrelease/2022/0228.html

視聴
https://www.tsujileaks.com/　「podcast - #セキュリティのアレ」

2 どうすればSASE導入に成功できる？ネットワーク検討　3つの盲点

SASE（Secure Access Service Edge）とは、あらゆる環境のユーザ／デバイスがクラウドサービスやデータに安全にアクセスできるよう、本社やデータセンターに通信を集約する従来の方法から、クラウドサービスへの経路上でネットワーク制御とセキュリティ統制を行なう方法へとシフトする考え方です。

SASEを構成する主要機能として思い浮かぶのが、セキュリティとゼロトラストネットワークです。しかし、クラウド活用を本当に促進するためには考慮が欠かせない3つのポイントがあります。詳細は、下記URLおよび無料配布中の小冊子で解説しています。ぜひご覧ください！

URL
https://www.iij.ad.jp/svcsol/campaign/sase_202010.html


IIJ
Internet Initiative Japan