

# 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.

August 2019

VOL.

153

政治家、元内閣総理大臣

特別対談 人となり

小泉 純一郎 氏

特集

オフィスITにまつわる  
お悩み解決





ぶろろーぐ 眠り病 / 鈴木 幸一 ..... 3

特別対談

人となり

政治家、元内閣総理大臣 小泉 純一郎 氏

IIJ代表取締役社長 勝 栄二郎

Topics

オフィスITにまつわるお悩み解決

お悩み 1 SaaS導入の観点から見た  
オフィスIT環境の課題を解決したい / 沖田 誠司 ..... 11

お悩み 2 オフィス・ネットワーク環境を整備したい / 吉田 賢矢 ..... 14

お悩み 3 エンドポイントセキュリティ対策を強化したい / 大野 慎吾 ..... 15

お悩み 4 快適なりリモートアクセスを実現したい / 吉田 賢矢 ..... 16

お悩み 5 ITインフラの運用に携わる人材不足を改善したい / 向平 友治 ..... 17

お悩み 6 クラウド利用時の認証管理を改善したい / 佐々木 直哉 ..... 18

お悩み 7 海外拠点のITインフラの課題を解決したい / 利光 健太郎 ..... 19

お悩み 8 基本的なセキュリティ対策を確実に進めたい / 久保 啓司 ..... 20

人と空気とインターネット インターネットで広がる新たなビジネスモデル / 浅羽 登志也 ..... 22

インターネット・トリビア 無線LANとWi-Fi / 堂前 清隆 ..... 24

グローバル・トレンド カリフォルニアでのデータ規制 / 飯塚 泰光 ..... 25

ライフ・ウィズセーフ シーサートに必要なこと / 齋藤 衛 ..... 26

ぶろろーぐ

眠り病

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



IIJを設立して以来、お盆休みをとったことがない。別にお盆休みを禁じているわけではなく、休みをとらないのは、私くらしいものである。振り返ってみれば、お盆休みをとったのは、サラリーマン生活を始めてから七、八年のあいだだけだった。

生来、あらゆる行動において怠惰な私だが、サラリーマンとなり、結婚をすると、お盆休みには必ず旅に出た記憶がある。上野から夜行列車に長いこと揺られて、東北の鄙びた温泉など、二度と行かないような場所、毎夏、奥さんの緻密な経費削減案にもとづく計画に従って旅をした。一年に一度の休暇となると、経費削減を前提としても、旅の案は広がって、肉体的には疲れ切るような旅程になる。お盆が明けて、オフィスに出勤する日には疲労困憊となっていて、仕事など手につく状態ではないのだが、その晩、仲間と飲み会などすると、翌日はすぐに元気になったものである。

IIJの創業以来、苦しい時期が長すぎたせいか、多忙でいつも疲労感があつたせいか、ほとんど休みをとらない習慣が身についてしまったが、昼間、オフィス

の机に頬杖をついて、居眠りをしていることも多い。休みをとらない、睡眠時間が少ない日常の欠陥をどこかで勝手に補っているのである。

今年株主総会が終わった翌日から、二〇日間近く欧州を回っていたのだが、出張の半ば過ぎの土日にイスの保養地に寄って、身体を休めようという計画が裏目に出たのか、ホテルに着くなり、眠り続けることになった。

チューリッヒの投資家にIIJの現状を説明して、夕暮れに保養地に着いた。元気であるという想定をもとに計画していたことを始めようと、部屋の机に資料を広げ、軽い食事をとりに行った。部屋に戻り、机に向かった途端、猛烈な眠気に襲われ、とりあえずベッドに横になった。それからが大変だった。部屋いっばいに明るすぎる高原の光が溢れるようになって、ベッドから出られない。目を瞑ると、あっとい間に眠っている。昼前になって、さすがにベッドから抜け出して、ホテルの食堂で珈琲を飲みながら、湖が広がる景色を眺める。目はあけているのだが、目覚めている

のかよくわからないまま、一時間ほど座り込んで、やっとの思いで部屋に戻る。ベッドに横になる誘惑には逆らうこともできず、ぼったりと眠る。次に目をあけると、すでに長い夏の陽が暮れている。慌ててルーム

サービスで軽い食事をとるのだが、またそのまま眠ってしまう。翌日もまったく似たような時間を過ごす。朝になり、資料をバッグに入れて、イタリアに向かう。条件反射なのか、その晩、イタリアで知人とディナーをする時には、目を覚まし元気がうだつたらしい。そのまま数日間は、慌ただしく知人や友人と話があつて、眠ってしまうことはなかった。初めてお目にかかったナポリの歌劇場のチャームिंगな総裁と食事をし、オペラの案内を受けた折も元気だったようだ。

帰りはフランクフルト経由で羽田に戻ったのだが、その便では離陸すると同時に眠り、着陸一時間前に起こされるまで眠り続けていたようだ。その後は、誰彼となく「眠り病に罹った」と喧伝していた。帰国後、二〇日を経て、ようやく「眠り病」が軽くなったようである。ほっとしているのである。

# 人となり

政治家、元内閣総理大臣

小泉純一郎氏



株式会社インターネットイニシアティブ  
代表取締役社長

勝 栄二郎

各界を代表するリーダーにご登場いただき、  
その豊かな知見をうかがう特別対談“人となり”。  
第16回のゲストには、  
元内閣総理大臣の小泉純一郎氏をお招きしました。

## 政治家を志すまで

**勝** 本日はお忙しいなかお時間を頂戴し、ありがとうございます。お酒を飲まない席でお話するのは久しぶりですね(笑)。

**小泉** 酒席以外では、音楽会くらいかな。  
**勝** では、さっそく始めたいと思います。小泉総理は政治家の家系に生まれ育ちましたが、ご自身でも小さい頃から政治家になろうという想いがあったのですか？

**小泉** いや、なかったね。高校生くらいまでは、まったく。政治家になろうと思ったのは、大学に入って、二十歳を過ぎてから。その頃、親父の選挙を手伝うようになった。それまではできるだけ目立たないようにしていた。嫌いなんだよ、目立つのが。しかし選挙が始まると、地元の人たちが仕事をしながら、朝早くから夜遅くまで手伝ってくれる。朝、街頭に立って一緒にお辞儀をしてくれたり、演説会の準備をしてくれたり……。自分の仕事があるのに、一生懸命やってくれる。そういう姿を見て、自分も手伝わなきゃいかんという気持ちになった。

当時は中選挙区制で、全候補者が集まる立会演説会があった。各候補者が一〇分くらいで政策を発表する。私の選挙区は定員四名だったから、結構いろんな話が出るわけだ。それらを聞きながら、さまざまに考えがあるんだなあと。それで政治に興味を持つようになった。

選挙中、親父が他の候補者の応援に行つて、地元を留守にすることがあった。そんな時は立会演説会に誰か代理を出さないといけない。ただ、知り合いの県議員や市議員を出すと、なんで〇〇が出るんだ？ということになるから、結局、身内が出ることになる。

**勝** そうなのですね。  
**小泉** 私は長男で、もう二十歳を過ぎていたから、お前が親父の代わりに演説しろと言っただよ。

**勝** まだ学生ですよ。  
**小泉** 学生だよ(笑)。これには参った。中学の時に弁論大会があった。一度、出されたことがあった。親父が選挙をやってるんだから、お前が出るよ。五分足らずの時間だったけど、まず学年ごとに演説して、その優勝者が集まって、さらに全校で弁論大会をやる。私は最上級生じゃなかったけど、一位になっちゃったんだよ！ 話上手じゃないかとかわれてさ。演説なんてそれ以来だった。

周囲からは「いずれは後継ぎだな」と見られていたのは事実だけど、どちらかと言うと引つ込み思案だった。しかし人間は変わるんだな。

大学に入ると活動的になってね。地元の(慶應)学生会の代表になり、いろんな行事で挨拶したり、三田会でOB会と折衝をやったり、会合などで話す機会も増えてきた。そうこうしているうちに、自分では目立つのはイヤだと言いつつも、目立つようになってしまった。同時に「政治は大事なんだ」という気持ちにもなってきた。

**勝** お父様は、政治家としての心構えとか、そういう話はされたのですか？

**小泉** それはいろいろ話したよ。この政治家はどうだとか、あの挨拶は長すぎだとか。とにかく話は簡単なほうがいい、原稿なんか見ちゃいかんと。それはよく言っていた。短く、わかりやすく、簡単にやれ。長いやつは飽きられるよ。今でもそれは心掛けてる。話は三分以内にとめる。結婚式で一〇分とか一五分やる人がいるけど、長いだろ？(笑)

**勝** そうですね(笑)。  
**小泉** そういことが親父の教えと言えれば教えだな。

## 落選、そして福田赳夫元総理の秘書に

**勝** 政界に入られてからの恩人ですとか、影響を受けた政治家はいらっしゃいますか？

**小泉** 福田赳夫先生。親父が福田派だったから、何かあったら福田先生を頼っていいよ。

実は、最初に出た選挙(一九六九年)で落選したんだよ。その選挙には、二七歳の新人世襲候補者が三人いて、ちょっと話題になった。小沢一郎さん、社会党の佐藤観樹さん、それと私。三人とも親父が衆議院議員で、同一年。当然、有利だったはずなんだ。その年の夏、親父が亡くなったことで、同情が集まる。知名度がある。若くて将来性がある。しかし、三人のなかで私だけ落選した。

**勝** そうでしたか。

**小泉** 落選したんだけど、一〇万票以上集めた。同じ選挙で一〇万票以上集めて落ちた候補者が私を含めて数人いた。群馬の小淵(恵三)さんなんて、三万票台で当選してるんだよ。おかしいよな(笑)。

**勝** 一票の格差ですね(笑)。  
**小泉** 落選すると、毎日選挙運動したつてしょうがないから、福田先生のところへ行つて「何か手伝うことはありませんか？」とうかがったら「私の秘書という肩書を使つていいから、陳情などあれば、持つてきなさい」とおっしゃつてくれた。ただ、その時「秘書」という肩書をもらつ



小泉 純一郎（こいずみ じゅんいちろう）  
1942年生まれ。神奈川県横須賀市で育つ。祖父、父ともに政治家。慶應義塾大学経済学部卒業。衆議院議員を12期務める。その間、内閣総理大臣、自由民主党総裁、厚生大臣、郵政大臣、農林水産大臣などを歴任。2009年に政界を引退。音楽鑑賞、映画鑑賞、歌舞伎ほか多趣味でも知られる。

い」と連絡があった。私は「出陣式（で司会をすること）の挨拶だろう」と思っていた。そして電話に出てみると、「すまん。立候補を辞退する」って言うんだよ！

**勝** あの出馬断念には驚きましたね。

**小泉** 出陣式の前日だよ。そこで突然「辞退する」って言うんだからさ。橋本 龍太郎さんが立候補することになったので、おそらく河野さんは勝てないと思ったんだろうな。

当時の雰囲気は、実績のある現職の（河野）総裁が無競争で再選されればいいという感じだった。しかし、橋本さんは新人（候補）だった。新人が無競争で選ばれるのはマズいって声が出始めた。ちょうどその頃、総裁選の方式が変わって、党員にも一票あげますということになった。党員に初めて投票権が与えられたんだ。それで「その一票のために党員集めをしていたのに、無競争では困る」ということになった。

急ぎよ、派閥の幹部に（出てくれないかと）頼んでみたが、断られた。そうこうしているうちに「小泉さん、出てくれないか」と来たわけだ。現職の河野さんが降りて、橋本さんが出るんだから、勝てるわけないよ。それに三〇人の国会議員の推薦がないと立候補できない。「そんな数の推薦人なんて集まらない」と思っていたら、「集めたらどうする？」って言うてきたので、「もし集まったら、その時に考えるよ」と返事した。そしたら本当に集めちゃったんだよね（笑）。つまり、総裁選を実行するために、私は担ぎ出されたようなもんだ。誰も（私が）勝つとは思っていない。「小泉さんなら、負けても傷がつかないだろう」って（笑）。

**勝** そんな舞台裏があったんですね。

**小泉** 結局、橋本さんが勝ったけど、一度（総裁選に）出ると、かなり注目されるようになった。

二回目（一九九八年の総裁選）に出た時は、最大派閥だった旧田中派（経世会）から小淵さんと梶山（静六）さんが出て、票が割れた。だから「今度はわからんぞ！」って言われたんだが、結果は最下位。しかも前回より票を減らした。これじゃあダメだと思った。

**勝** 小淵政権、森政権は比較的短命の政権になりました。

**小泉** 森（喜朗）さんが辞めることになった時、また私に出ろって言うんだよ。でも「二度あることは三度ある。総裁選で二度も負けているおれを担いでも、また冷や飯だぞ」と。ただ、周りがそれでもいいって言うんだよ。それで今度こそ最後と決めて立候補した。

いざ、街頭演説会に出ると、すごい聴衆なんだよ。有楽町でも、大阪でも。渋谷なんか、ハチ公前を人が埋め尽くして、車も何も通れない。

その勢いに乗って当選しちゃった。

**勝** あの「小泉フィーバー」は凄かったですね。

**小泉** 私は総裁選に三回出たけど、自分から手を挙げたことは一度もない。出ると言われて、出た。そして「また負ける」と思った三回目も当選するんだから、不思議なもんだよ。

### 内閣総理大臣として改革を断行

**勝** 内閣総理大臣として長期政権を築き、全く新しい政治の在り方、手法を実現されました。数多い実績の一例として、行財政改革、構造改革、特殊法人改革、経済財政諮問会議、歳出削減、日米外交重視、拉致問題解決、自衛隊の海外派遣……などがあります。なかでも一番力を入れた政策は何でしたか？

**小泉** やはり郵政民営化には力を入れた。自民党内にも反対が多かったし、野党は全て反対だった。私が総理になれば郵政民営化は実現できると言って、総裁選を戦った。

郵政民営化法案は、自民党内から造反が出たが、衆議院は僅差で可決。しかし参議院で否決された。普通ならあれでおしまい。参議院で否決されたのだから、内閣総辞職が当然と言われた。

私は「国民の信を問う」ために、衆議院を解散したのだが（いわゆる「郵政解散」、考えてみれば、参議院で法案が否決されて衆議院を解散したところで、参議院は変わらないんだから（法案成立は）むずかしい。さらには、自民党が勝ったって、何度でも（参議院で）否決してやる。なんてバカなことをするんだ、非常識だと言われた。たしかに非常識なんだよ（笑）。参議院で否決されて衆議院を解散するなんて。しかし、郵政民営化を焦点に選挙をやったら、圧勝したんだよ。

**勝** 解散する時の記者会見も非常に印象に残っています。

**小泉** うん、実はあの会見は、酒気帯び会見だった（笑）。目玉の法案が否決されたあと、すぐに臨時閣議を開いて、解散を決定。その記者会見を夜八時から聞くことになった。

あの頃、年に数回、経済界の要人と食事を催していて、たまたまその日に会があった。経団連会長だったトヨタ自動車の奥田（碩）さんとか、キヤノンの御手洗（富士夫）さんとかね。それなのに「今夜、記者会見をやりますから、（食事は）キャンセルして」お弁当を用意します」って言うんだよ。しかしね、財界の人たちだって、わざわざ何カ月も前から予定を入れている。国会を解散するといっても、まだ現職の総理なん

て何もしないのは、申し訳ないとも思った。

当時、福田先生のお宅には、朝からすごい数のお客が来ていた。七時頃、門が開く前から外で待っている。大物政治家っていうのは、毎朝こんな感じなのかと。一方、私は肩書だけは秘書といっても、何をしたいのかわからない。じゃあ、お客が多い早朝に、玄関番とか電話番号でもやらせてもらおうと思いついて、朝四時に起床して、七時前に福田邸に着いて、お客の対応をしたんだ。福田先生は早い日は八時に出るけど、普通は九時くらい。それまでお客の取り次ぎや、スリッパを出したり、靴を揃えたり……まあ、下働きだな。そうして福田先生が出かけたあと、地元に戻って、選挙運動をしたわけだ。

今、振り返ると、最初に落選して良かった。途中で落選すると、ブランクが空くから。あと、選挙というのは、普段が肝心だと痛感した。日頃の活動が大事だと。

**勝** なるほど。

**小泉** 選挙前に大方が見て「当選確実」というくらいでないダメなんだ。

**勝** 事前に票は読めるものですか？

**小泉** 読めない。票は読めない。

**勝** そうなのですね。

**小泉** だいたいの雰囲気だよ。だから地元の選挙運動は熱心に行った。それでだんだん認められて「若いんだから、一回くらい落選しても心配するな」と激励された。そのお陰で二回目からは落選せずに当選できた。

### 三度目の正直だった自民党総裁選

**勝** 二〇〇一年、内閣総理大臣に就任されましたが、総理になるまでの道程もけっして順風満帆ではなかったようですね。

**小泉** そう。自民党の総裁選挙で二度敗れて、（総裁になった）三度目も「当選は無理だ」って、応援してくれた人でさえ思っていたからね。

**勝** そうでしたか。

**小泉** 初めて総裁選に出たのは一九九五年。社会党の村山（富士）さんが総理の時で、自民党の総裁は新自由クラブから戻ってきた河野（洋平）さんだった。それで九月に総裁選に向けた選対会議があって、私は河野さんの出陣式で司会をやることになっていた。いよいよ明日が出陣式という日、河野さんから「あとで電話するから、事務所にいてほし

## 人となり

特別対談





だから、会には出席しなければならない。だから「六時からの懇談会には出るよ」と言つて、彼らと食事をしたんだ。

場所はニューオータニだったと思う。一室に二〇人ほど集まつていて、食事が用意されている。すると旨そうなツマミが出てくるんだよ。「ちよっと酒がないとさびしいなあ。一杯だけ出してよ」つて(笑)。それで飲みながら話をしたわけ。「もうじき記者会見じゃないですか、お酒は控えたほうがいいですよ」つて言われたけど、「絶対に赤くならないから大丈夫」つて(笑)。酒が入っていたなんて、気づかなかつたでしょう？

勝 ええ、まったく。会見の内容は、前もつて考えておられたのですか？

小泉 そりゃ考えたよ。否決されたあと、多少時間があつたからね。短く、順序だてて、簡単にメモして、こういう記者会見をしようと。だから原稿はナシ。

勝 原稿ナシですか！

小泉 うん、項目だけ見ながら喋つた。かえつて酒が入つていて良かったかも(笑)。

勝 そうかもしれませんね。

小泉 あの時、野党は「自民党は造反が出て、分裂」「選挙も勝ちだ」と思つたらしいね。自民党が勝つと思つたのは少数派だった。だから、あの閣僚が聞きに来たよ、「本当に解散するんですか？ 勝てると思いませんか？」つて。私が「やつてみなきゃわからん」と言つたら、青くなつていた(笑)。

郵政民営化は、国民がダメと言うなら諦めるけど、(国会が)当たり前

の法案を反対するなんて、どうしても納得いかなかつた。会見の翌朝、街頭に立つた若手議員が「びつくりしました！」つて言うんだよ。外で拡声器が使えるのは朝八時からだから、早朝のラッシュアワーの駅で彼らはマイクなしで挨拶する。それが、あの朝に限つて、普段は見向きもしないで駅に入っていく人たちが「あんた自民党か？」つて聞いてきて、「自民党です」と答えると、「お！ 頑張れよ。小泉、頑張れ！」つて握手してくれた。それでびつくりしたつて言うんだよ。こんな初めてだつて。そんな追い風に乗つて選挙をやつたら、圧勝しちゃつた。あの記者会見が効いたのかもなあ。

勝 そうですね。そう思います。

### 拉致問題解決に向けて

勝 拉致問題についてもうかがわせてください。北朝鮮から五人の拉

## 人となり

特別対談

小泉 これは人間の考えが変わる一つの典型だな。日本には資源がほとんどないし、石油も輸入に依存している。だから私が総理だつた頃は、エネルギー政策を考えると、原発は不可欠というのが、役所でも経済界でも常識だった。実際、二〇一一年の時点で、日本には五四基の原発があり、そのうち約四〇基が稼働して、全電力の約三〇パーセントを供給していた。

二〇一一年の地震と津波、あれは想定外だったかもしれない。しかしよく調べてみると、当時から日本の原発は安全対策が十分じゃないという議論もあつた。想定を超えた事態が起こるかもしれないという意見はあつたんだよ。ところが、原発推進論者や電力会社は、そんな大きな地震はこない、津波もこない、きたとしても安全対策は十分と主張していた。ところが、あのメルトダウンだよ。

私は二〇〇九年に政界を引退した。そして事故のあと、原発に関する本を読み始めた。かつて経産省をはじめ、原発推進論者は、日本の原発は安全で、他の電力に比べてコストが安い、二酸化炭素を排出しないクリーンエネルギーだと主張し、挙げ句の果てには、永遠のエネルギーを謳つて「もんじゅ」までつくつた。

国会が設置した事故検証委員会で委員長を務めた黒川清先生とたまに話をするんだ。この前、会つた時に「福島原発が爆発したのは、地震が原因だとか、津波が原因だとか、いろんな議論があるけど、いったいどっちなんですか？」と尋ねた。すると、はつきり言つたよ。「あの事故は自然災害ではありません。人災です」と。では、なぜ人災なのか？ 「安全対策が十分じゃなかつた」。

福島では幸いにも四基目は爆発せずにすんだ。しかし万が一、四基目が爆発していたら、福島から半径二五〇キロ圏内の住民は避難しなければならなかつた。二五〇キロ圏内というと、東北全域に加え、東京・神奈川も含まれる。そうなるとうんざりな五千万人が避難だよ！ これは最悪の状況。原発がひとたび事故を起こすと、多くの人が故郷を失ふことになる。現に今でも帰れない人が何万人もいる。それで私は「日本に原発は要らない」と考え、講演を始めたんだ。

勝 原発はテロ対策なども大変らしいですね。

小泉 そう。だからコストが安い、安全つていうのはウソ。事故前は原発一基作るのに五千億円かかつていたが、今では安全対策などを含めると一兆円以上になる。あと、原発はクリーンエネルギーつていうのもウソ。使用済み核燃料を捨てる場所がないんだから。産業廃棄物、いわゆる一般のゴミだよ、それを処分する会社をつくらうとしたら、処分場を

致被害者が帰国できたことは、良い意味でサプライズだったと思うのですが、そこはある程度、行かれた時点で確証があつたのですか？

小泉 いや、全くなかつた。

勝 そうだったのですか！

小泉 田中均さんという外務審議官が秘密裏に接触を重ねて、下準備を進めてくれたんだよ。実態のわからない北朝鮮を相手にね。今の將軍の親父さんがトップの時だった。

勝 金正日ですね。

小泉 あの頃、アメリカのブッシュ大統領が「悪の枢軸」と呼んで、今にも北朝鮮を攻撃しかねない雰囲気だった。すると、田中さんが北の高官とやり取りするなかで「小泉総理が来れば、(金正日が)会うと言っている」と、側近から返事があつたつて言うんだよ。来てくれれば、必ず会うと言っていると。じゃあ行つてみようかというところで、朝早く発つて、日帰りで行くことにした。

勝 賭けではありませんね。

小泉 うん、そう。どうなるかわからない。あの段階では、拉致被害者の名前も少しはわかつていたけど、何人いて、誰が生きていて、誰が亡くなつていいのか、多くは不明のままだった。未だに正確な数はわからない。実際に行つた結果、返してくれることになつたけど、帰れなかつた人のほうが多い。帰国後の記者会見では、いろいろ叩かれたよ。

勝 そうでしたね。

小泉 自民党の議員まで批判したからね。でも、国民のあいだでは「行つて良かった」という意見が多かつた。

勝 アメリカには事前に連絡したのですか？

小泉 もちろん。けど、よく秘密が保たれたと思うよ。あとから聞いた話では、田中さんも外務省内部から「何も知らせなかつた」と批判されたいらしい。それくらい秘密裏に進めたから、情報が漏れなかつた。田中さんみたいな人がいたから、向こうも交渉に応じた。あれは極秘折衝でないとダメだっただろうな。

勝 そうですね、本当に。

### 「脱原発」を掲げる

勝 総理をお辞めになられたあと、二〇一一年に東日本大震災が起り、原発事故が発生しました。それを機に「脱原発」の方向に転じられました。

確保しない限り、都道府県知事が許可を出さない。それなのに、もつと危険な核のゴミを出している原発企業はなぜ認められているのか？ 私にはそれが不思議でしょうがないんだ。

### 向上心を持ち続ける

勝 最後に若い人に向けたアドバイスの言葉をいただけますか。

小泉 若い人に限らず、万人にとつて大事なのは「向上心を持つこと」「学び続けること」だよ。所詮、人間の知恵なんて微々たるもので、知らないことがほとんどだ。私も原発がこんなに危険だということは、自分で勉強して初めて知つた。歳をとつた人でも、若い人はなおさら、知的なことでも肉体的なことでもいいから、自分を向上させようという心を持つことが大事なんだよ。社会に出た時、何を学べばもつと自分の能力を高めることができるのか、そういう学ぶ気持ちだな。これはどんな人にも必要だと思う。

江戸時代の国学者・佐藤一斎が非常にいい言葉を残している。

少而学 則壯而有為

壯而学 則老而不衰

老而学 則死而不朽

少くして学べば、則ち壯にして為すことあり

壯にして学べば、則ち老いて衰えず

老いて学べば、則ち死して朽ちず

勝 なるほど。こんな言葉をよく見つけられましたね。

小泉 本が好きだからね。これは誰にとつても大切なことだよ。学ぶこと、向上心は。

勝 その通りですね。

小泉 「もうおれは死ぬんだから、何でもいじやないか」ではなく、努力し続け、知的好奇心を持ち続ける。これを知ると、人生面白いよ。

勝 若い人だけじゃないですね。

小泉 そう。老いて学べば、死んだ後も朽ちることはないつていうんだから！ これは名言だよ。

勝 本当に見事な言葉ですね。本日は、貴重なお話をどうもありがとうございました。



1  
お悩み

# SaaS 導入の観点から見た オフィスIT環境の課題を 解決したい

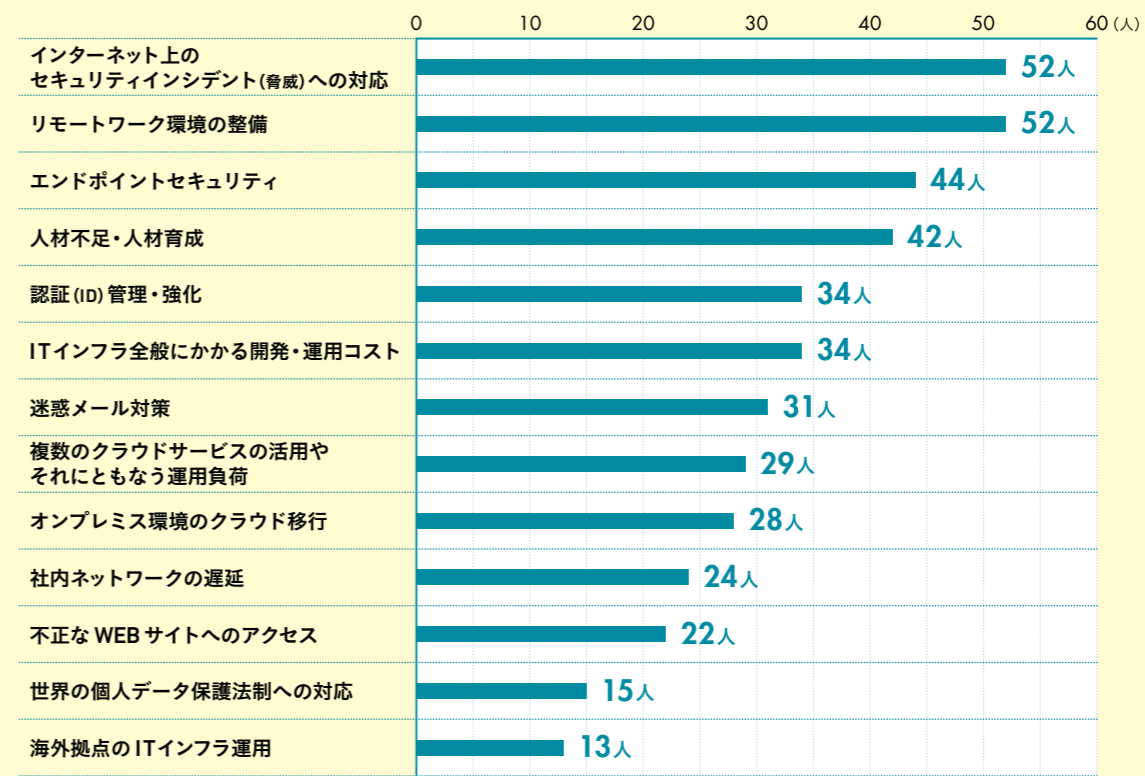
生産性向上・働き方改革への取り組みの一環として、  
オフィスIT環境におけるSaaS導入が活発化している。  
しかし、導入を担当する情報システム部門は、SaaSの導入によって生じる  
新たな課題と既存の課題の優先順位の決定に頭を悩ませている。

IIJ 執行役員  
プロフェッショナルサービス第一本部長

沖田 誠司

# オフィスITにまつわる お悩み解決

小誌が実施している読者アンケートで、  
オフィスのIT環境にまつわるお悩みを調査。  
そこから浮かびあがってきた課題は、生産性向上や働き方改革への対応をはじめ、  
リモートワーク環境の整備やセキュリティ対策など多岐にわたる。  
今号の特集では、皆さまからいただいた  
オフィスITにまつわるお悩みの解決策を探る。



組織のITインフラにまつわるお悩み(複数回答可)

実施：2019年2月20日～3月31日まで(2019年2月発行号のIIJ.news vol.150) 回答人数：156人

## 活性化する企業のSaaS利用

ビジネスの成功・成長に向けたさまざまな企業活動が試みられるなか、日本では近い将来、「人手不足」が大きな問題になると見られています。それに対し、企業規模にかかわらず、生産性向上・働き方改革といった対策が進められています。

二〇二〇年夏の東京オリンピック・パラリンピックの折りには、国内外から観戦客が首都圏に集中し、主に都心部におけるビジネス活動に影響が出ると予測されています。そこで、時差出勤、在宅勤務、あるいはビジネス活動の縮小といった対応が迫られるとともに、その影響を最小化して事業継続性を維持することが喫緊の課題となっています。

こうした背景もあって、企業内システム・ネットワークの老朽化対応、関連会社の統合、分社化によるIT環境の見直しなどを機に、情報系SaaSの本格的な利用を始めるケースが増えています。

代表的なSaaSとしては、マイクロソフト社のOffice365があります。同社のクラウドシフトの戦略もあり、同サービスが日本リージョンでスタートした五年ほど前から、先進的な大企業は活用を開始し、最近では中小企業にも広がりつつあります。Office365は、従来のメール、スケジューラに加え、TV会議、リアルタイムコミュニケーション、ファイルシェアなど、生産性を向上させるための迅速な情報共有機能を備えています。

セールスフォースの国内展開も堅調で、(実は、IJも導入した一社なのですが)国内における浸透率はますます高まっています。同社のサービスはCRM(カスタマー・リレーションシップ・マネージメ

ント)として活用されることが多いのですが、同じ仕組みをERM(エンプロイ・リレーションシップ・マネージメント)に応用することで、従業員エンゲージメントを向上させ、人材確保につなげるという狙いも持っているようです。

このようにソフトウェア業界がクラウドシフトすることで、顧客が自前導入するという選択肢は減少しており、自社でシステムを構築しなくていい、持たなくていい、運用しなくていい、どこからでも使える……等々、SaaSの利用は、自前導入に比べて多くのメリットをもたらしてくれそうです。企業のニーズに機敏に対応することができているSaaSの利用は、これから進んでいくでしょう。

## 変わることから生まれる三つの課題

SaaSが提供する機能・利便性は企業にとって非常に魅力的である反面、課題もあります(ただこれは、決してSaaSが原因というわけではなく、情報システムそのものの在り方が変化していることにもない、システム全体にも変化が求められているという意味です)。

### ● アクセス遅延

第一にSaaS向けのインターネットの接続速度、トラフィックの増大により、企業のインターネットへの経路にボトルネックが生じて、アクセスの遅延を引き起こすことです。

その解決方法として紹介されることも多い「ローカルブレイクアウト/インターネットブレイクアウト」は、「拠点やエッジデバイスからインターネットに直接出て行けばいい」と誤解されている向きもあります。しかし、正しくは「信頼するインターネット



報を活用できるようになり、企業活動が活発化します。それに合わせて、セキュリティの守備範囲を広げ、強化するクラウドデザインが必須になります。つまり、SaaS利用が、情報活用を活性化するとともに、セキュリティを見直す契機となるのです。

最近の傾向として、セキュリティのコントロールポイントとなる「抑止」「予防」「検知」「回復」のうち、「検知」「回復」を重視するお客さまが増えて、「攻撃の高度化により、従来型の「予防」では対応しきれなくなっているため、検知機能を高度化し、速やかな判断とアクションにつなげることが求められているのです。さらに「検知」については、外部からの攻撃への対策効果だけでなく、その取り組みを社内にも周知することで、内部犯行を「抑止」する効果も期待できます。

加えて、セキュリティ上の適切な利用をコントロールするCASB(Cloud Access Security Broker)にも触れておきます。現時点で本格的にCASBを導入できるのは、あるべきSaaSの利用形態、セキュリティ観点からの対策優先度、現状のセキュリティ対策などが十分に整理されているケースに限られます。その理由は、同じCASBとカテゴライズされているテクノロジは、実現形態が、一様でなく、それぞれ長所・短所があるため、コストともマッチしたものを選択するには、SaaSの利用方針(何を許可/禁止し、何に対して、何をモニタするのかなど)が定まらないと選択しきれないからです。

CASBの具体的な導入にあたって、利用者のSaaS通信をモニタする方式を選ぶことになった際は、モニタ可能なネットワーク設計でなければなりません。ちなみにこの場合、先に触れたローカルブレイクアウト/インターネットブレイクアウトに関して、拠

アクセスを、ボトルネックとなり得る箇所から迂回する」ことであって、拠点やエッジデバイスでも迂回できますが、従来からのセンター側でも迂回は可能です。どの手法が一番いいのか? といっても、一律の「解」があるわけではなく、最終的にはコスト効果で評価します。例外的に日本国内のセンターを経由している海外拠点に対して、レイテンシ向上(遅延の解消)が目的に加わる場合、拠点・エッジデバイスで迂回する選択肢が有力になります。しかしその際も、最終的には拠点の業務、サイズ、使われ方に対するコスト効果で評価することになります。

IIJはMicrosoft Azure/Office 365への閉域接続サービスと合わせて、Office 365の導入・移行インテグレーションにも注力しており、多くの導入実績を重ねています。こういった案件では、ほぼ100パーセント、ネットワークの見直しをセットで実施していますが、大手企業でもセンター側のボトルネック迂回で落ち着いているケースが大半です。理由は拠点・エッジ側に仕組みを広げると、お客さまの管理負担が追いつかなくなるためと考えられます。

#### ●AD連携

第二にSaaSアカウントの管理負担の問題があります。オンプレミスのExchangeサーバであれば、社内のActive Directory(以下、AD)との連携が行なわれますが、Office 365の利用となると、直接社内ADと連携させるわけにもいかず、連携用のAD環境が必要となります。加えて、お客さまのモチベーションとして「せっかくSaaS(クラウド)を使うのだから、アカウント連携もクラウドで」と、所有しないことへの要望もあって、AD連携部分もクラウド化を強く望む傾向があります。二〇一八年、IIJがADのサービスを開始したところ非常に好評であることから、管理者に

点・エッジデバイスからインターネットに迂回する選択に制約が加えられる点には留意が必要です。

また、スマートデバイスの利用が増えていることから、紛失リスクに対する「予防」としてMDM(Mobile Device Management)によるデバイス管理の導入は、もはや当たり前になりつつあります。デバイス管理という観点から、最近では統合エンドポイント管理(UEM)により、PCを含むあらゆるデバイスを効率的に一括管理するのが主流になっており、企業のPCのWindows 10化が先行しているお客さまにおいては、検討が具体化し始めています。

#### 一貫性のある解決が望まれる

このようにSaaS導入にともなう課題に対処するテクノロジは広範に及び、効果的な相互作用を持たせながら対応しなければなりません。そのため、情報システム部門は、こういった課題の検討にどこから着手すべきなのか? 検討がまとまらない……といった悩みを抱えています。大企業の情報システム部門は、SaaS管理者、ネットワーク管理者、セキュリティ管理者、端末管理者など、各々の利害を総合的に加味しながら対応する必要がある一方、中小企業では、数少ないシステム管理者が複数の問題を把握・処理するのは非常に困難になっています。

こうした課題解決は数年前なら、インターネット回線、インターネットGW、WAN、LAN、セキュリティと、それぞれ個別の案件としてご依頼いただくことがほとんどでしたが、最近ではそれらを、まるっと「ネットワーク」と総称して、ご相談いただくことが多くなっています。

それに対してIIJは、ワンストップで課題対

とって日常的なADサーバ管理の負担が重く、アウトソースへのニーズが高いことがうかがわれます。

アカウント管理の観点からもう一つ、Office 365だけの利用であれば、AD連携のみですませるケースが多いですが、Office 365以外のSaaSも合わせて利用する場合、SaaSによるユーザ利便性を向上させることに加えて、インターネット上のサービスであるSaaSのユーザ管理、パスワード管理を、SaaS毎に行わなければならないようになります。この負担軽減は、管理者だけでなく、ユーザからも要望されるので、統合認証の仕組みが欠かせません。また、これは単なる負担軽減だけでなく、ユーザ退職時のアカウントの停止などもまとめてタイムリーに行なうことで、不正利用へのリスク低減にもつながります。

大企業では、統合認証の仕組みを社内システム向けに導入していることがありますが、クラウドとの連携を想定していなかった時期に導入されたものは、社内の統合認証との連携が敬遠されると同時に、統合認証の仕組みもクラウドで提供されることを求める声が多いのは、ADと同様の傾向と言えます。

#### ●セキュリティ

第三にSaaS利用により「どこでも使え、仕事ができる」ことから、社外利用されるデバイスの紛失、ウイルス感染などによる情報漏えい対策が不可欠となります。SaaS利用による生産性向上・働き方改革の一環として、リモートワーク環境も並行して整備されることが多いのですが、働き方の多様性に合わせてエンドポイントセキュリティの重要性が、いっそう高まっています。

これは「SaaSを導入したから、セキュリティをこうしたほうがいい」という話ではありません。IT活用により、場所・時間に縛られず、より多くの重要な情報にあたることを第一とし、お客さまとのパートナーシップにもとづいて解決に取り組んでいます。例えば、大企業であれば、事業形態・ITの利用形態が多様であるため、クラウドデザインに対するコンサルティングから始めたり、中小企業であれば、全体を網羅したソリューションを検討・提供したりしています。

#### 人材力をイノベーション領域へ

冒頭でも触れた通り、人材不足が(特にIT分野では)深刻化しつつあります。それが特に顕著なのはITを使ってビジネスを展開している企業のイノベーション、業務改革、業績向上などを推進していくためのリソースです。本稿で取り上げたIT領域は情報システムであり、今後も技術革新などを通して生産性向上を後押ししてくれるでしょうが、それはいわゆる「インフラ領域」における話であって、企業に独自性をもたらす「イノベーション領域」に対する寄与とは性格を異にします。

IIJは二〇一五年に「OneCloud」というネットワーククラウド構想を発表しました。今では、大手も含めて多くの企業が、ここで紹介した課題に対する解決策として、我々が提供する情報系ネットワークをクラウド化したサービスを導入しており、構想は現実のものになりつつあります。

IIJはこれからもインフラ領域における有効なサービスをより多く提供していくことで、企業の情報系システムをサポートして生産性向上を実現するとともに、企業の人材力をインフラ領域から解放して、イノベーション領域に振り分けられよう、微力ながら貢献していきたいと考えています。

お悩み

3

東京オリンピック・パラリンピックを控え、政府は開催期間中の交通混雑を緩和するため、首都圏を中心にテレワークの導入を推進しています。また、期間中の混乱に乗じたサイバー攻撃やその後を見据えた戦略として、企業と取引先などを含めたサプライチェーン全体のセキュリティ強化に向けたガイドラインの策定や、中小企業におけるセキュリティ対策水準の引き上げなどを重点項目に掲げています。

一方、攻撃者の活動は組織的かつ高度化しており、取引先の担当者になりすまして、一見、普段と変わらないメールを送りつけて多額の現金を振り込ませる

## エンドポイントセキュリティ対策を強化したい

働き方の多様化やサイバー攻撃の高度化を背景として、ユーザの水際で脅威を退ける「エンドポイントセキュリティ」が注目を集めている。ここではその概要を紹介する。



IIJセキュリティ本部  
先行戦略室長  
**大野 慎吾**

### セキュリティ担当者の悩み

「ビジネスメール詐欺」や、マルウェア（実行ファイル）を使用することなく、パソコンのOSの標準ツールである PowerShell を悪用した「ファイルレスマルウェア攻撃」など、環境変化や既存対策の間隙を突く手口でユーザを狙っています。

こうした働き方の多様化や、攻撃手法の高度化などに對して、セキュリティ担当者は限られたコストと人員リソースで、どのようにセキュリティを確保すればいいのか、頭を悩ませているのではないのでしょうか？

### 再評価される エンドポイントセキュリティ

IJでは、クラウド環境を導入することで、物理機器の管理コストを削減できるといった利点が謳われていますが、実際にはオフィス・ネットワークの見直し・増強や、プロキシを迂回させるためにPACファイルによる除外設定の運用、ロードバランサなど新たなオンプレミス機器の導入が必要になります。そのため、総合的なコスト・メリットが薄まり、クラウドサービスの導入が本末転倒の結果を招く可能性も否めません。以上のことから、クラウドサービス

「社内ネットワークの入口で強固に守る」という従来の考え方を見直す必要が出てきます。

新たなセキュリティ対策技術が現れると、攻撃者はそれを回避する新たな攻撃手法を生み出すというイタチごっこが繰り返されてきましたが、マルウェア感染を100パーセント防ぐことはむずかしいという認識が一般的になっています。実際、企業のセキュリティ担当者からも「既存の対策をすり抜けてマルウェアに感染してしまった」、「原因究明に時間がかかる」、「原因が特定できないので、対応が応急処置になっている」という声を多く耳にします。

そのような状況において、シグネチャを用いずA

IJでは、ISPならではの強みや運用ノウハウを生かして、クラウド環境下でのインターネット接続を考慮した最適なオフィス・ネットワークを提案しています。課題解決のポイントは「振り分けの自動化」と「インターネット接続環境の分散」です。

「IJクラウドプロキシサービス」は、頻繁に更新されるOffice 365の宛先情報を自動で取得・更新することで、PACファイルの除外設定などの運用負担を軽減します。さらにOffice 365を除くポート80（HTTP）／443（HTTPS）に向けた通信をプロキシ宛てに転送したり、Office 365宛てを指定したインターネット接続環境に転送したりすることで、トラフィックを分散できます。

また、企業ネットワークに必要な機能を仮想化してクラウド上で提供するSDN/NFVサービス「IJ Omnibus」では、Office 365やWEBフィルタリングを通さずに、直接、インターネットへ接続する経路も用意し、負荷の高い通信をクラウド上で振り分けて快適なネットワーク環境を実現します。

IJは、クラウドサービス導入によって変化するインターネット・トラフィックの流れに、最適な接続環境と拠点間ネットワークを提供しています。今後も、お客さまのクラウド環境に最適なオフィス・ネットワークをサポートしてまいりますので、どうぞご期待ください。

### 振り分けの自動化と インターネット接続環境の分散

IJでは、二〇一八年秋、既知あるいは未知のマルウェアに対する防御、流入時の原因調査、再発防止などを実現する「アンチウイルス」と「IT資産管理」の機能を組み合わせた「IJセキュアエンドポイントサービス」をリリースしました。

このサービスでは、マルウェアの検知・隔離だけでなく、アンチウイルスとIT資産管理を統合したポータルサイトを提供しており、マルウェアの検知状況を管理画面に表示し、簡単な操作で原因となるユーザの行動を特定・対策して再発を防ぐことができます。また、クラウドサービスであることから、管理サーバの構築・運用・更新作業などが不要で、必要な機能に必要な台数分だけ契約できるので、導入コストと運用負担を減らせます。

エンドポイントセキュリティを取り巻く市場環境は著しく変化しており、この先一二年でさらに製品のコモディティ化が進むと見られています。IJでは、最新の動向・技術をいち早くつかみ、お客さまの安全な業務環境を実現するために、サービスの拡充に努めてまいります。

お悩み

2

## オフィス・ネットワーク環境を整備したい

クラウドサービスの導入によりオフィス・ネットワークのトラフィックの流れが変化しますが、そこで生じるいくつかの課題に対して、どのような解決策が考えられるだろうか？

IIJ サービスプロダクト事業部 営業推進部  
ネットワークソリューション課

**吉田 賢矢**



### オフィス・ネットワークの環境変化

総務省の統計調査データ「平成30年通信利用動向調査」によると、企業におけるクラウドサービスの利用率は、毎年堅調な伸びを示しており、昨年度は調査対象の約六割に迫っています。

また、昨年からはオフィス・ネットワーク周辺では、二〇一八年九月三〇日にメーカーサポートが終了したNotes 8.5と、二〇二〇年一月一四日にサポートが終了するWindows 7の移行が話題になっています。そしてWindows 7の移行先として注目されているのが、生産性向上に役立つ最新機能を搭載したOffice 365

一般には、クラウド環境を導入することで、物理機器の管理コストを削減できるといった利点が謳われていますが、実際にはオフィス・ネットワークの見直し・増強や、プロキシを迂回させるためにPACファイルによる除外設定の運用、ロードバランサなど新たなオンプレミス機器の導入が必要になります。そのため、総合的なコスト・メリットが薄まり、クラウドサービスの導入が本末転倒の結果を招く可能性も否めません。以上のことから、クラウドサービス

IJでは、ISPならではの強みや運用ノウハウを生かして、クラウド環境下でのインターネット接続を考慮した最適なオフィス・ネットワークを提案しています。課題解決のポイントは「振り分けの自動化」と「インターネット接続環境の分散」です。

「IJクラウドプロキシサービス」は、頻繁に更新されるOffice 365の宛先情報を自動で取得・更新することで、PACファイルの除外設定などの運用負担を軽減します。さらにOffice 365を除くポート80（HTTP）／443（HTTPS）に向けた通信をプロキシ宛てに転送したり、Office 365宛てを指定したインターネット接続環境に転送したりすることで、トラフィックを分散できます。

また、企業ネットワークに必要な機能を仮想化してクラウド上で提供するSDN/NFVサービス「IJ Omnibus」では、Office 365やWEBフィルタリングを通さずに、直接、インターネットへ接続する経路も用意し、負荷の高い通信をクラウド上で振り分けて快適なネットワーク環境を実現します。

IJは、クラウドサービス導入によって変化するインターネット・トラフィックの流れに、最適な接続環境と拠点間ネットワークを提供しています。今後も、お客さまのクラウド環境に最適なオフィス・ネットワークをサポートしてまいりますので、どうぞご期待ください。



5 お悩み

# ITインフラの運用に携わる 人材不足を改善したい

本稿では、ITインフラにフォーカスし、ITインフラの運用工数削減と、生産性向上に向けた解決策を提案する。

IIJ サービスプロダクト事業部 営業推進部  
クラウドソリューション課

向平 友治



## 運用対象を減らすクラウド活用

ITに限らず、多くの業界で人手不足が課題となっており、従業員一人当たりの業務量は増加傾向にあります。また「働き方改革」に象徴されるように、長時間労働に対する問題も広く認知されています。そして、これら二つのテーマを解消するには、生産性向上の実現が不可欠と言えます。

一方、ビジネスモデルが多様化・高度化するにつれ、一社あたりのシステムの数は増える傾向にあります。システムと一口に言っても実際は、サーバなどのハードウェア、WindowsなどのOS、そのうえで動作するアプリケーションやミドルウェアなど、いくつも

4 お悩み

# 快適なリモートアクセスを 実現したい

リモートワークの実現に不可欠なのが安定したネットワークだが、条件によっては、切れやすく、つながりにくいこともある。ここでは、そうした問題を飛躍的に改善するIIJフレックスモビリティサービスを紹介する。

IIJ サービスプロダクト事業部 営業推進部  
ネットワークソリューション課

吉田 賢矢



## リモートワークの課題

従来からニーズのあった「リモートワーク環境」ですが、公衆Wi-Fiの普及やシェア・オフィスの利用拡大により、これまで以上にニーズが高まっています。しかし、ネットワークの品質については、「切れやすい」「つながりにくい」といった課題の改善がほとんど見られていません。

例えば、外出先からWEB会議に参加した際、映像がカクつき、音声が届かずに会議が滞ってしまった経験を持つ人は少なくないでしょう。また、海外出

張などで現地のモバイル端末やWi-Fi環境を利用して社内イントラにアクセスした際、ネットワークの遅延が原因で思った通りに仕事が進まなかったこともあるのではないのでしょうか。

## IIJフレックスモビリティサービス

IIJは二〇一八年末から、従来のリモートアクセスサービスとは全く違う、切れずにつながり続ける(VPNを利用した)クラウド型リモートアクセスサービス「IIJフレックスモビリティサービス」を提供しています。普段の外出時や移動中、海外出張時のWi-Fi環境など、インターネット接続環境が不安定なときにも、社内イントラへのアクセスが快適になり、クラウド型のグループウェアサービスを利用する際の業務効率を飛躍的に改善します。

また、海外でのインターネット接続環境や距離によるパケットロスが原因で発生するアプリケーションの再接続・再ログインの必要がないため、国内と同レベルの業務効率を維持できます。

IIJフレックスモビリティサービスではWindowsログオンと連動し、VPNのON/OFFを自動的に制御する設定が可能です。管理者は、ユーザが勝手にVPN切断することを禁止できるため、リモートデバイスのセキュリティレベルを保つことができます。さらに、自社内のネットワークを自動的に検知し、VPNをOFFにするポリシー設定が可能のため、リモートアクセスユーザはVPN設定を全く意識することなく、社外・社内を問わず、安全に社内リソースにアクセスできます。

近年、タブレットやスマートフォンを業務で使用する機会が増えており、そうした端末のWEBセキュリティが課題になっています。IIJフレックスモビリティ

ティサービスでは、ポートによる宛先制御が可能です。例えば、ポート80(HTTP)/443(HTTPS)はプロキシ宛てといったポリシーを設定できるため、PACファイルを設定できない端末でも、WEBアクセスのセキュリティポリシーを適応可能です。

## アーキテクチャ

### NetMotion Mobility

これらの機能は、ネットモーションソフトウェア社のNetMotion Mobilityによって実現されています。リモートアクセスユーザのデバイスにNetMotion Mobilityクライアントというエージェントをインストールすると、仮想ネットワークインスタンス(仮想NIC)が構成されます。デバイスのアプリケーションは仮想NICと通信します。Wi-FiやLTEのインターネット接続が切れるといった理由で実IPアドレスが変化した場合でも仮想NICはActiveなため、アプリケーションはネットワークが切れていないと判断し、セッションを保持します。

また、不安定な無線を利用したインターネット接続環境下での一般的なVPNサービスは、TCPパケットの不達による再送信で通信遅延が生じます。それに対しNetMotion Mobilityは、UDPプロトコルを利用することで、TCPで生じていたパケットの再送信が発生しない仕組みと、パケットのハッシュ値を計算・再構成しパケットの多重化を工夫して確実に届くように制御する機能を実装しています。こうして、これまでは「頻繁に切れたり、つながりにくかった」リモートアクセス環境を快適にします。

現状のリモートアクセス環境に不満をお持ちの方は、ぜひ一度、IIJフレックスモビリティサービスをご検討ください。

のコンポーネントが連動して一つのシステムとして機能します。

システムの運用には、コンポーネント単位で異なる考慮ポイントや作業が必要となりますが、一般的にこの分野には人手を要する作業が数多く残されており、「システムが増える→運用コンポーネントが増える→運用者の負担が増加する」という構図になることが多いのが実情です。

そこで、まずは運用対象となるコンポーネントを減らすことができれば、工数の低減が図れます。現在はIaaSやSaaSなどのクラウドサービスにより、ハードウェアやOSの運用をサービス提供者に委ねるケースも増えており、それだけで運用工数を大幅に削減できます。実際、クラウド活用は、運用工数削減の有力な選択肢の一つとして広く普及しており、IIJでも「IIJ GIO」というブランドでIaaSを提供しています。

## 自動化による工数削減

クラウドの活用によって管理対象レイヤが減るとはいえ、特にIISの場合、稼働している仮想サーバ自体の運用は利用者の責任範囲となりますし、さまざまな理由でクラウドを採用できないシステムも一定数存在します。従って、コンポーネントを減らすアプローチに加え、残った工数を削減することも検討しなければなりません。

IIJもアウトソーシングサービスを提供している事業者として、クラウドや物理機器に対する運用工数の増大に悩んでいたのですが、その解決策として「運用をできるだけ自動化し、現場を楽にしよう」

というコンセプトのもと、「IIJ統合運用管理サービス(UOM)」というクラウドサービスを開発し、自社でも活用しつつ、お客さまにご利用いただけるサービスとしても提供しています。このUOMは、特徴的な機能としてシステムで発生した事象に対し、あらかじめ指定した操作を自動で行なう「自動オペレーション機能」を搭載しています。

システムのエラーのなかには、運用ナレッジが溜まってくると、「このエラーはあのサービスを再起動することで直る」とか、「このログを取得すれば原因追究できる」といったように、ある程度対処方法が見えるものが少なくありません。UOMはこれを利用して、該当するエラーが発生した際、指定したスクリプトを自動で実行します。それにより、典型的な対処はシステムが自動で実行してくれるので、運用工数を低減できるのです。

システム運用の世界では、このような定型作業であっても、あらかじめ定められた手順書に沿って、人間が手作業で行なうケースが数多く存在します。IIJもこの定型業務による運用負荷の増大に悩まされてきました。そこで、UOMを自社でも利用して運用を自動化し、それまで手動で行なっていた作業の約半分を削減しました。

さまざまなビジネスシーンで業務効率化が叫ばれるなか、工数の半分を削減できる領域はそう多くないと思われがちです。「システムは利用できて当然」という認識が強いこともあり、通常、運用の現場を意識することは少ないかもしれませんが、それだけに効率化の余地が多く残されているとも言えます。IT業界の人手不足解決の一策として、クラウド化と運用の自動化を検討してみたいかがでしょうか。

## クラウド利用時の 認証管理を改善したい

本稿では、クラウド利用の増加とともに複雑かつ煩瑣になりつつある「認証」に関する課題を見つうえて、有効な解決策を紹介する。

IIJ サービスプロダクト事業部 営業推進部  
セキュリティソリューション課

佐々木 直哉



### クラウド全盛時代の新たな課題

「クラウド全盛時代」と言われて久しい昨今、Office 365やG Suiteをはじめとしたグループウェアだけでなく、さまざまな機能がSaaSとしてクラウド提供されています。それにとともに、今までオンプレミスでやっていた認証管理と同等レベルの機能がクラウドにも求められるようになりました。ここでは、これらの課題と解決方法について考えていきます。

### 煩瑣になった「認証」

クラウドを利用するうえで、認証に関する課題は、二つに大別されます。  
近年、クラウドの利用は増加の一途を辿っており、複数のサービスを用いている会社も増えてきました。

そこで出てきたのが一つの課題である、クラウドサービスのID基盤/SSO(シングルサインオン)基盤への対応です。  
そもそもオンプレ環境では、認証サーバやID管理製品、SSO基盤で一元的に管理していたものが、クラウド化されることで、ID/PWの更新を個別に行なわなければならない、新規ユーザの登録や退職者のID削除といった業務が増えます。また、ユーザ目線からも、各クラウドへ異なるID/PWでのログインが必要となり、利便性が低下します。すなわち、今までオンプレ環境で行なっていた一元的な管理が行なえなくなっているのです。

二つ目の課題は、ID/PWの漏えいリスクが高まることです。オンプレ環境での認証と違い、クラウドへのログインにはフィッシング攻撃などの危険がともないます。そして、ユーザのID/PWが漏えいすると、自社の情報が流出するリスクも高まりますし、一つのクラウドのID/PWが漏えいすることで、それを用いたアカウントリスト攻撃により、他のクラウドへの不正ログインや情報流出の恐れも出てきます。これらは、ユーザが多くのID/PW管理に対応しきれず、同一または類似のID/PWを使用しがちであるために起こる問題です。

### 適切な解決策は？

以下では、それぞれの課題について、解決策を紹介いたします。  
まず一つ目のID基盤/SSO基盤への対応に関しては、AD(Active Directory)を基点としたID基盤連携や、SSO基盤連携と各種クラウドとの認証連携というアプローチが考えられます。

現状、あらゆるクラウドにID管理が実現できるID基盤は存在しません。そうしたなか、ADを基点「現地で運用サポートをアウトソースする」のいずれかです。  
まず一つ目の「日本からの遠隔管理」ですが、それに適したツールは多数存在しますし、IIJでもいくつかのサービスを提供しています。例えば、システム運用を効率化するSaaS型サービス「IIJ統合運用管理サービス(UOM)」や、資産管理のSaaSサービス「Lanscope Caron GIO」などです。UOMは海外のサーバ類を国内と合わせて監視したいケースにおいて、Lanscope Carは海外のクライアントPCを遠隔管理したいケースなどにおいて、ご利用いただいています。

しかし、これらの管理ツールで解決できるのは一部の課題に過ぎず、海外拠点の多くの課題が一足飛びに解決するわけではありません。日本よりも安定しないインターネット環境下でどのようにITシステムを構築するのか？ IT担当者がいないかPC操作などに関する社員からの質問にどう対応するのか？ 万が一、機器が故障した場合の対処は？ 等々、想定される課題は多岐にわたります。  
そこで、二つ目の選択肢「現地で運用サポートをアウトソースする」が、より現実味を帯びてきます。これは、お客さまの理想としては「海外現地法人のITに関するさまざまな課題に「フレキシブル」に対応してほしい」ということになるでしょう。この点についてもIIJグループは、世界に広がる海外拠点を活用して、さまざまな提案を用意しています。

### IIJによる海外拠点のサポート

IIJグループでは、ほぼ全拠点に日本人スタッフを配置しており、お客さまからのリクエストが多い、次のようなご要望に対応してきた実績があります。

とした各サービスへのID連携により、ID管理の負荷を下げることは可能です。また、各種クラウドとの認証連携を行なうSSO基盤を作ることで、認証をまとめることができます。  
二つ目のID/PWの漏えいリスクについては、認証の統一化、多要素認証の導入というアプローチが考えられます。  
そもその原因となるID/PWが漏えいするポイントを抑えること、そしてID/PWが漏えいしたときでも情報流出を起させないようなプロセスの認証を求めることが有効な対策になります。具体的には、クラウド用のSSO基盤を用いることで、ID/PWの漏えいのポイントを抑えられます。また、ワンタイムパスワードなどの多要素認証による本人確認を行なうことで、ID/PWが漏えいしても、情報流出を未然に防ぐことができます。  
このように、クラウド側で足りない部分を別サービスによってカバーすることが今後、必要になってくると思われます。

### IIJのアプローチ

IIJではこれらの課題に対するアプローチとして「IIJ IDサービス」を提供しています。同サービスはOffice 365をはじめとしたクラウド利用に際して、ADを基点としたID連携や各種クラウドとの認証連携の機能を実現し、さらに、自身の認証時に多要素認証を加えることもできます。そのほかにも、ADログオンを基点とした統合Windows認証機能とWindows Helloなどを組み合わせることで、パスワードを実現することも可能です。

このように、ID/PWの漏えいによる情報流出から自社を守るという観点に立ち、クラウドへの認証アプローチを再検討してみたいかがでしょうか。

- 問い合わせを日本語と現地語で受けてほしい
- IIJの現法で依頼をお受けして、日本人が日本語で、現地スタッフが現地語で対応。
- お客さまのIT担当者に代わって、PC操作に関する問い合わせや機器故障に日本語と現地語で対応。
- 予算規模の少ない現地法人を低コストでサポートしてほしい
- 平日の日に電話受付を限定することで費用を圧縮
- 作業が発生するたびに対応する「チケット制」のご提案。
- 海外拠点のIT環境がどうなっているのか把握したうえで運用を依頼したい
- IIJの現法スタッフがお客さまの海外事務所を訪問し、調査を実施。
- ネットワークだけでなく、PCのライセンス一覧を作成するなど、必要な情報を可視化。

海外拠点のサポートでもっとも重要な点は、日本のように厳格な運用体制を構築するのではなく、お客さまのご要望と予算に応じて、最善の策を講じていくことです。その際、海外現地法人だけでなく、日本本社の要望も加味しながら対策を検討していくことも重要です。

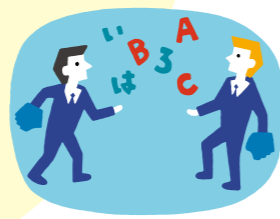
IIJグループでは、日本の営業・技術担当者、現法の営業・技術担当者が日頃から密接に連携して、お客さまのサポートにあたっています。お客さまの日本本社と各国の現法が良好な関係のもとビジネスを遂行できるよう、IIJグループの知見を最大限に活かして、必要かつ最適なITインフラを提案します。また、近い将来、日本で運用しているサポートセンターを海外にも拡張して、二四時間・多言語で電話サポートするなど、お客さまの幅広いご要望にも応えていきたいと考えています。海外のITインフラの構築・運用でお悩みの際は、お気軽にご相談ください。

## 海外拠点のITインフラの 課題を解決したい

日系企業の海外展開が進むと同時に、各拠点のITインフラを維持するための人材確保が課題になっている。  
ここでは、そうしたサポートをアウトソースする方法を中心に解決策を見てみたい。

IIJ グローバル事業本部  
グローバル営業部長

利光 健太郎



### 海外拠点の課題をどう解決するのか？

二〇一九年現在、IIJはアメリカ・イギリス・ドイツ・中国・シンガポール・タイ・インドネシア・ベトナムの八カ国・一都市に海外拠点を展開しており、世界の主要なビジネスエリアでITソリューションを提供しています。

特にこの二三年は、日系企業の海外現地法人のITインフラに関する相談や問い合わせが増えていますが、担当者のお話をうかがうと、ほとんどの企業が「海外拠点に専任のIT担当者を置くことができない」という共通の課題をお持ちのようです。

これに対する解決方法は、大きく分けて二つあります。「海外拠点を日本から遠隔管理する」もしくは

7

お悩み

6

お悩み

お悩み 8

# 基本的なセキュリティ対策を 確実に行ないたい

さまざまなサイバー脅威が溢れるなか、忘れてはならないのは「基本的な対策を実行しておくこと」である。本稿ではIIJのサービスを参照しながら、セキュリティ対策の基本を確認する。

IIJセキュリティ本部 セキュリティビジネス推進部  
インテグレーション課

久保 啓司

## 組織を取り巻くサイバー脅威

ランサムウェア、標的型攻撃、個人情報漏えいなど、さまざまなサイバーセキュリティ事故・事件が報道されています。サイバーセキュリティに携わる者として「少し脅かし過ぎでは？」と思う反面、実際に発生してしまったインシデントの現場で対応にあたる時、「もっと警告しておくべきだったか？」とか、「事前にアドバイスできることがあったのでは？」と反省することしきりです。

た日数の中央値は二〇四日と報告されており、気づくことが非常にむずかしい攻撃であると言えます。ビジネスメール詐欺は、国際的な取り引きを行なうある企業において、巨額の被害が出た事案が報道されたり、日本語を使用したビジネスメール詐欺も報告されるなど、まだまだ被害の拡大が懸念されています。

ランサムウェアについても、攻撃の入り口が多様化しており、不正な添付ファイルを使用したメールやウェブサイトからの感染だけでなく、最近では、インターネット経由のリモートデスクトップで不正アクセスし、ランサムウェアを実行させるといった高度な攻撃も現れています。

## 脅威への対策

では、ここに挙げたような脅威に対して、どのような対策をとるべきでしょうか？ 各々の脅威に特化した対策もあると思いますが、新たに出てくる脅威に対して付け焼き刃で右往左往するよりも、基本的な対策をしっかりと行ない、何か不審なことがあればすぐに気づき、迅速に対応できる体制を整えておくことが重要です。

IIJでは、これらの脅威に対する基本的な対策として、左記のようなサービスを提供しています。

- メールやウェブなど組織に入ってくるコンテンツのセキュリティの確保
- IIJセキュリティMXサービス
- IIJセキュリティWebゲートウェイサービス
- IIJセキュリティWebゲートウェイサービス
- 境界防御(ファイアウォールなど)を利用したアクセス制御
- IIJマネージドファイアウォールサービス

## 情報セキュリティ10大脅威

(2018年に発生した社会的影響が大きかった事案)

順位	脅威	前年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW*
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開にともなう悪用増加	4位
10位	不注意による情報漏えい	12位

\*初めてランクインした脅威

こうした状況のなか、組織のシステム管理者の方は「自分の組織の対策は十分か?」「インシデントが発生したら、どう対応すればいいのか?」「前回発生したインシデントの対応は間違いなかったか?」「……等々、悩みは尽きないと思います。

IPA(情報処理推進機構)は毎年、大きな影響を及ぼした情報セキュリティの脅威を「情報セキュリティ10大脅威」として発表しています。ここでは「個人」と「組織」という異なる観点からそれぞれの脅威を順位付けしていますが、今回は「組織」の脅威について見てみたいと思います。(右表参照)

## セキュリティ10大脅威

最新の調査では「標的型攻撃による被害」、「ビジネス

- 端末のセキュリティの確保(エンドポイントセキュリティ)
- IIJセキュリティエンドポイントサービス
- Cyberance導入支援ソリューション

メールやウェブコンテンツのセキュリティを確保することで、一部の標的型攻撃のメール、不審なビジネスメール詐欺、ランサムウェアによるウェブへの誘導などに対する対策が可能になります。

次に境界防御ですが、組織の業務システムがクラウドサービスやSaaSなどの外部サービスを多用している昨今、システム・ネットワークの境界が曖昧になりつつあります。そこで、組織の根幹となる情報の管理サイトと外部との境界で適切なアクセス制御・監視を行なうことが重要になっていきます。

端末のセキュリティの確保(エンドポイントセキュリティ)では、発生してしまったインシデントへの対応を端末で検知・対応できるEDR(Endpoint Detection and Response)の提供を検討しています。

これらの対策を組み合わせたうえで、横断的かつ相関的にログを解析し、どの段階まで攻撃が進行しているのかを分析すれば、実際の脅威の重要度を判断できます。そして実際にインシデントが発生した際には、その発生源を複数のログから追跡し、被害の拡大を食い止められます。

IIJCSOCサービスは、この機能を実現するサービスです。多層防御でアクセス制御している複数の対策機器のログを相関的に分析し、発生した不審なログから実際の脅威の重要度を判断し、アラートとしてお客さまにお知らせします。実際にインシデントが発生した際は、その発生源を複数のログから追跡し、被害拡大を防止する機能を提

スメール詐欺による被害、「ランサムウェアによる被害」がトップ3を占めました。前年の順位と比べると、順位は多少入れ替わっているものの、この三つの脅威がトップ3で、組織にとって不動の脅威として継続していることがわかります。その一方で四位には「サプライチェーンの弱点を悪用した攻撃の高まり」という新たな脅威も入ってきました。

標的型攻撃は、二〇一六年からIPAの10大脅威の一位にランクされ続けている脅威で、国内では某研究組織などが長期にわたり侵入されていたという事案も報じられています。

FireEyeのレポート「M-Trend2019」によると、二〇一八年、アジアパシフィック地域の組織では、外部からの指摘で侵害を検知した割合は四一パーセント、また、セキュリティ侵害の発生から検知までに要し

供します。

## サイバーセキュリティの「かかりつけ医」

このように考えていくと、組織のサイバーセキュリティにおける基本的な対策は、どんな脅威に対しても大きな違いはありません。これは私たちの身体の健康対策と似ているかもしれません。いろいろな病気の脅威がありますが、健康であることの基本は「適度な運動・適切な睡眠・適切な食事」を確保することです。そのうえで実際に調子が悪くなったとき、気軽に相談できて、普段から様子を見てもらっている「かかりつけ医」を持つておくと、大きな安心につながります。

IIJのセキュリティエンジニアは、組織ITのサイバーセキュリティの「かかりつけ医」でありたいと考えています。例えば、IIJCSOCサービスは二四時間三五五五、組織のネットワーク・システムを見守り、不審な点が見つかれば通知し、不安があれば相談いただけるサービスです。

またIIJでは、最新のサイバーセキュリティに関する情報を収集し、観測データにもとづいたインターネット上の攻撃の傾向やセキュリティ事案を「WizSafe Security Signal」「IIR」「IIR-SEC Tプログラム」などで公開・発信しています。自組織の対策を検討される際、これらを参考情報としてご利用いただければと思います。

多くのサイバー脅威にさらされながらも、萎縮することなくITという技術フルにご活用いただける環境を提供したい——それがIIJセキュリティエンジニアの願いです。



人と空気とインターネット

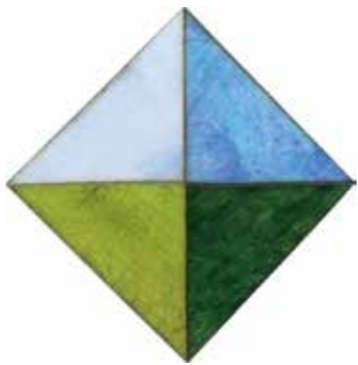
## インターネットで 広がる

### 新たなビジネスモデル

「イー・イーノ」バージョンインスティテュート

取締役

浅羽登志也



巨大プラットフォームによる

寡占が進む一方、創意工夫を凝らした、

新しいビジネスモデルも健闘を見せている。

今回は、そんな事例を二つ紹介する。



先日、とあるイベントに参加するために、初めて WeWork に行ってきました。WeWork は、アメリカ発祥のコワーキングオフィス (Coworking Office) の提供会社です。共用デスクでも東京では月額六万円以上、専用デスクは要相談と、他のシェアオフィスサービスよりも割高ですが、二〇一八年二月、六本木にオープンした日本最初の拠点は、開業前に九割以上の席が売れてしまうという大盛況だったそうです。二〇一八年中には都心五区八拠点で約四万平米を借り上げるまでに急成長し、市場から新築オフィスビルの空室在庫を払底してしまったとも言われています。現時点で、東京に(近日オープンも含めて)二一拠点、横浜一拠点、名古屋一拠点、大阪三拠点、神戸一拠点、福岡二拠点と、地方も含めてすごい勢いで拠点を展開しています。

WeWork には机と椅子、鍵付きキャビネット、Wi-Fi や有線 LAN、業務用プリンタ、電話ブースなど、オフィスに必要なものは一通り揃っています。そのうえ、カジュアルでポップな雰囲気が特徴的で、天井は黒塗りの打ちっ放し、広い共用ラウンジにはカラフルなソファやテーブルが置かれ、ラウンジを囲むように並んだ会議室はガラス張り、無料ドリンクコーナーにはコーヒーマシーンやビールサーバーもあります。魅力的なのは雰囲気だけではなく、私が参加したような交流会や、スタートアップのピッチイベントからヨガ教室など、さまざまな催しが開かれ、会員同士の交流も図られています。さらに、各拠点には会員企業間のマッチングやイベントの企画運営を担当する「コミュニティマネージャ」も常駐していて、会員同士の交流を促進しています。

契約は一カ月単位なので、ゼロからオフィス環境を構築・維持するより、WeWork との短期契約を好むテナント企業が増えているそうです。利用者は、個人事業主やフリーランス、学生、子育て世代、副業者など、多様な人々が集まっています。顧客企業の規模や業種別にカスタマイズしたビジネスサービスも提案できるのではないのでしょうか。例えば、「御社もそろそろマネージメント教育など始めてはいかがですか?」とか、「〇〇社は、御社くらいの規模のとき、こんな人事評価制度を導入して、社員のモチベーションアップにつなげて成長されています」など、EC サイトのレコメンデーションのような、企業にとって便利なサービスが揃って、さまざまな業種・規模の企業に対するコンサルティング・ノウハウが蓄積されていくため、もう顧客企業は「WeWork から離れない!」なんてことにもなるかもしれません。

「Google や Amazon のような巨大プラットフォームには追いつけない!」なんて諦めないで、IT 以外の領域に目を向けると、プラットフォームになれるチャンスが転がっているかもしれません。

#### 「パン・アキモト」の挑戦

話は変わりますが、先日読んだ本で紹介されていた小さなパン屋さんのビジネスモデルがとてもユニークかつ感動的だったので、紹介します。

那須塩原にある「パン・アキモト」という家族経営のパン屋さんなのですが、「三年間保存可能なパンの缶詰」を開発し、世界中に届けているのです。パンの缶詰を作ろうと思ったキツカケは、阪神淡路大震災のとき、パンを支援物資として送ったのに、必要としている人にうまく配給できず、そうこうしているうちにカビが生えて食べられなくなったという苦い経験があったそうです。その後、紆余曲折を経て、柔らかくて美味しいパンを三年間いつでも食べられる「パンの缶詰」の開発に成功し、日本、アメリカ、台湾、中国で特

業主やスタートアップばかりでなく、大企業がプロジェクトで活用したり、アメリカでは IBM や Amazon のような大企業が WeWork のオフィスを一棟借りするケースも出ているそうです (WeWork の発表によると、全会員の約二〇〜三〇パーセントが一〇〇人以上の大企業とのこと)。さらに、We Membership という会員サービスのもと、IT サービス、研修・教育、保育所、福利厚生、社会保険など、多種多様なサービスが提供されています。

#### クラウド・オフィスの誕生!?

ところで、WeWork のサービスのあり方をよく考えてみると、これは「オフィスのクラウド化」と言えます。ビルやオフィスフロアというインフラをまとめて借りるなり所有するなりして、そこに必要な機器や什器、基本サービスを設けて、デスクやスペース単位で顧客に月額提供するというビジネスモデルは、まさにクラウドコンピューティングで言うところの IaaS サービスです。コミュニティマネージャやその他諸々の付帯サービスも受けられるので、PaaS や SaaS も用意されていることとなります。

このようなプラットフォームビジネスには、顧客企業に関する情報も蓄積されていくはずですが、コミュニティマネージャのサービスなどは便利なので、顧客に関する情報がどんどん溜まっていくでしょう。だからこそ、マッチングサービスができるわけです。そのよ

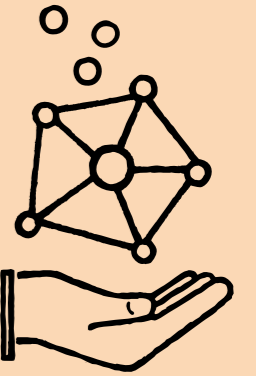
許も取得したそうです。

ここまでなら普通 (と言うと大変失礼ですが) なのですが、さらにすごいのは、パンの缶詰の「リユースシステム」を構築している点です。この缶詰は「保存食」という位置付けなので、企業や自治体などが災害対策の名目で購入するケースが多いそうです。リユースシステムを考案した動機は、ある自治体から「税金で購入したもので、職員に配って食べるわけにもいかず……」期限が切れた缶詰を引き取って処分してほしい」と言われたためでした。そこで思いついたのが、次の購入を約束してくれるなら、賞味期限の半年前に古いものを引き取って、新しいものに入れ替えるという下取りシステムだったのです。下取りした缶詰は「ハンガーゼロ」(日本国際飢餓対策機構) という NGO に引き渡して、海外の飢餓地域に支援物資として送ってもらいます。引取りまでの経費はパン・アキモトが負担し、そこから先は NGO が寄付金などでまかなう仕組みだそうです (このリユースシステムは、今では個人の顧客も利用可能とのこと)。小さなパン屋、パン・アキモトは、経営は苦しいながらも、なんとかビジネスとしてこの仕組みを回して頑張っているようです。

最近、浅間山が不穏な動きをしているので、私も非常食として購入してみようと思っています。自分の購入したパンの缶詰が、将来、自分で食べることにならずとも、世界のどこかでお腹を空かした子供達に届けられると思うと、なんだかうれしいではないですか! これも一つのシェアのあり方だと思います。

これからは、ネットで主流になったクラウドやシェアリングなどの新たなビジネスモデルをうまく現実世界にも展開していく流れが増えるのではないかと感じました。

# Internet Trivia



インターネット・トリビア

## 無線LANとWi-Fi

皆さんのご家庭でも、オフィスでも、パソコンをネットワークにつなぐとき、LANケーブルを使うことが少なくなっていないでしょうか？ 特に家庭ではLANケーブルをつなぐより、「無線LAN」のほうが普及しているかもしれません。実際、家庭用のインターネットサービスでレンタルされる機器には最初から無線LANの機能が搭載されていたり、そうでなくても数千円程度で「無線LANのアクセスポイント」を手でできます。以前はイマイチだった通信速度も改善され、日常的な利用には支障ありません。

ところで、こういった無線LANのことを「Wi-Fi」と言うことがあります。実は「無線LAN」と「Wi-Fi」には使い分けがあることをご存じでしょうか？

「無線LAN」「WLAN(Wireless LAN)」は特定の技術を指すのではなく、ケーブルを使わないLAN全般を指す言葉です。ただ、各メーカーの製品が勝手バラバラだと不便なので、共通の規格に沿った製品を作ることが一般的です。

現在使われているのは、IEEEという国際的な電気・電子関連の専門家団体によって定められた通信規格で、担当する802委員会ワーキンググループ11の名前をとって「IEEE802.11」というシリーズ

で呼ばれています。IEEE802.11シリーズのなかには利用する電波の種類(周波数や無線技術)によっていくつかのバリエーションがあり、「IEEE802.11g」や「IEEE802.11a」などと名付けられています(製品のパッケージは「11g」や「11a」と省略形で書かれることも多いようです)。「無線LAN」と言えば、ほぼこのIEEE802.11シリーズの通信規格に対応したものを指すと考えていいでしょう。

では、「Wi-Fi」とは何でしょうか？ これを説明するには、無線LAN対応製品の登場直後のことを振り返る必要があります。二〇〇〇年前後に無線LAN機器が市販されるようになった直後は、その製品がIEEE802.11シリーズに対応していると表示されていても、メーカーが異なると正しく通信できない場合があります。新規格に沿った製品が出始めた頃にはよくあることで、規格が曖昧でメーカーによって解釈が違っていたり、規格制定のタイミングでは想定されていなかった課題があとから見つかったりするためです。

こうした状況は無線LAN普及の妨げになるので、有力メーカーが集まって互いの製品が通信可能か試験

I I J M V N O 事業部  
事業統括部 シニアエンジニア

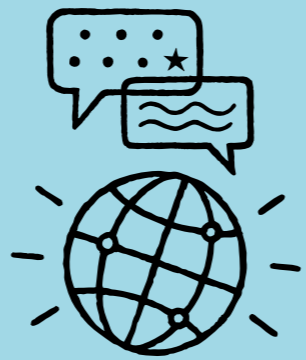
堂前 清隆

して、認定を与える団体を立ち上げました。この認定を通った製品に表示されるのが「Wi-Fi」(Wi-Fi CERTIFIED)という名称とロゴです。Wi-Fiロゴが表示されている商品であれば、メーカーが異なっても通信可能なのが確認されており、購入者は一定の安心感が得られます。

ロゴを認定する団体は、当初は Wireless Ethernet Compatibility Alliance (WECA) と名乗っていましたが、現在は Wi-Fi Alliance に改称しています。

なお、Wi-Fi はあくまでも「Wi-Fi Alliance の試験をパスした」という印です。Wi-Fi 表記やロゴの使用は、Wi-Fi Alliance によって制限されていますが、IEEE802.11シリーズの規格自体は公開されているため、Wi-Fi ロゴがない製品でも、IEEE802.11シリーズ対応機器として利用できますし、Wi-Fi ロゴがある製品とも通信可能です。実際に市場を見ると、最新の機器でも Wi-Fi ロゴを表示せず、「IEEE802.11シリーズ対応無線LAN機器」としてメーカー独自の試験を経たうえで販売されているものもあります。こうした機器も実際の利用には支障ありませんが、厳密な意味ではこれらを「Wi-Fi」と呼ぶのは正しくないということになります。

# Grobal Trends



アメリカにおけるスポーツ中継の面白さは、プレーの質以外にデータ提供の多彩さによるところも大きく、例えば、ニューヨークヤンキースの野球中継で、投手と打者との対戦成績に加え、打球方向の傾向と守備位置をマップして、その傾向通りの打球でアウトになると、データの有効性が視覚的にわかるわけです。今年からMLBはデータ提供をAWSから受けているので、アナウンサーが「powered by AWS」と連呼しています。昔なら大手コンピュータメーカーの役割を、今はクラウド事業者が担っているのです。

昨年、EUで施行されたGDPRは、アメリカのクラウド事業者へのEUのヒステリックなヒガミだろうと大西洋越しに見ていましたが、昨年のfacebook騒動などを見ると、オプトアウトの権利など正しい防衛策だったとわかります。事業者による行き過ぎたデータ収集と、そのマネタイズに対する静かな怒りがアメリカでも徐々に広がっているようです。

そうした流れのなか、来年一月よりカリフォルニア州で消費者プライバシー法(CCPA)が施行される予定です。当初、この話を聞いたとき、カリフォル

グローバル・トレンド

## カリフォルニアでのデータ規制

I I J America Inc. President & CEO

飯塚 泰光

ニアはテック企業のお膝元だし、シリコンバレーの大企業は膨大な資金でロビー活動をしているので、政治家の茶番では？と個人的には感じました。ところが報道によると、この法律は市民の提案からスタートし、最終的には議会が引き取り、知事が署名したそうです。引き金はやはりfacebookと英Cambridge Analytica社の騒動だ……。市民のなかには、裏切られたと感じた人もいたのではないのでしょうか。便利で、しかも無料のサービスにはわけがあることが明らかになった今、ユーザの信頼を取り戻すために、事業者には厳しいルールへの対応と透明性の確保が求められるはずです。

カリフォルニア州のみならず、アメリカで個人情報扱うには大きな注意が必要な時代になります。そもそも事業を行なう側はおざなりにしてはいけなかったはずで、ルールが明確になっただけ、とも言えます。我々は、その点をわきまえてお客さまをサポートさせていただくとともに、響きは古いですが、電気通信事業者の自負と謙虚さをもって、今後の事業を進めていきたいと考えています。

カリフォルニアの空は青く高い。I I J America LA オフィスが入居するビル。



<b>株式会社 インターネットイニシアティブ</b>	
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 3F 〒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
新潟営業所	新潟県新潟市中央区東大通 1-3-1 帝石ビル 4F 〒950-0087 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
沖縄営業所	沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル 8F 〒900-0015 TEL:098-941-0033

#### IIJグループ／連結子会社

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 エンジンアリング  
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 7F  
〒101-0041 TEL:03-5205-4000

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

株式会社 IIJ イノベーションインスティテュート  
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:03-5205-6501

株式会社電巧社ネットワークス  
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:03-5205-6766

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

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

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153

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」編集部  
〒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  
表紙イラスト／末房志野  
デザイン／榎原健祐 (Iroha Design)  
印刷／株式会社興陽館 印刷事業部

# Information

## Lead Initiative 2019 開催のご案内

IIJグループは、法人のお客さまを対象にしたイベント「Lead Initiative 2019」を開催します。“インターネットでビジネスを前に”をテーマに「ネットワーク」「クラウド」「セキュリティ」の最新トピックスや、これからの企業情報システムを支えるテクノロジーをご紹介します。

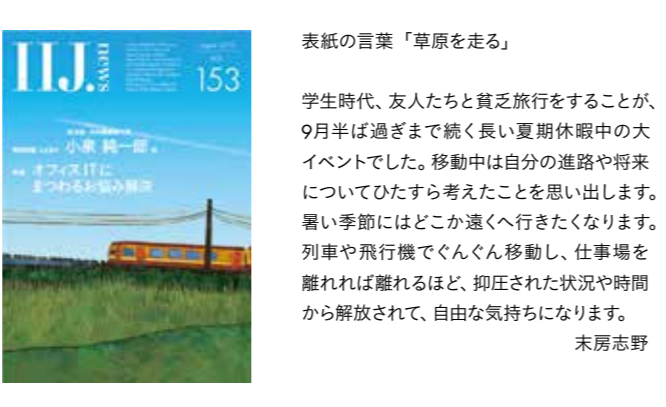
**日時：**  
2019年10月23日(水) 13:00～17:30 (開場 12:00)

**会場：**  
セルリアンタワー東急ホテル (渋谷区)

**参加費：**  
無料 (事前登録制)

詳細・申し込みはこちらから  
https://www.iij-lead-initiative.jp/

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153



●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ください。URL: https://www.iij.ad.jp/iijnews/

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153

編集後記

猛暑が一気に押し寄せてきましたね。暑さのため、休日もなるべく外出は控えるのですが、あるイベントにIIJが出展することになり、休日返上で参加してきました。いろんな出展があるなか、ドローンの展示が目につきました。子供たちがドローン进行操作するのを眺めているら、ふと、ドローンはどんなふうに浸透していくのだろう? と思いました。近い将来、手荷物を運んだり、道案内してくれるような機能が搭載されるかもしれません。暑いときには、頭上から扇風機として頭を冷やしたり、日傘の役割をはたしてくれるかもしれません。多機能化すれば、スマホのように1人1機の時代が到来し、誰もが好みにあったドローンを保有し、相棒のような存在になるかもしれません。そこら中を飛び回るドローン同士がぶつかるという問題も起きそうですが、散歩中の犬の喧嘩をキッカケに飼い主同士が恋に落ちるなんてことがあるように、ドローンで始まる恋がうまれるかもしれません。公園で出会った男女が「そのドローン、かわいいね」などと会話するシーンをイメージしたところで、子供が操作するドローンは障害物にぶつかり、地面に落ちたのでありました。(K)

## wizSafe

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153

ライフ・ウィズセーフ

## シーサートに必要なこと

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153

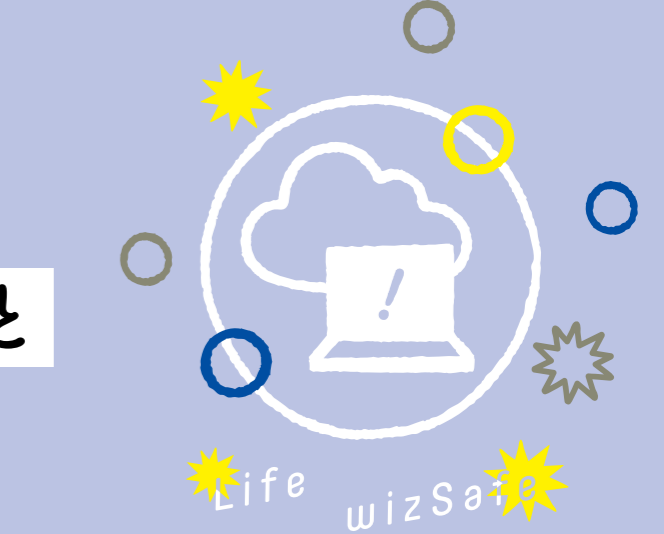
IIJ セキュリティ本部長  
**齋藤 衛**

サイバー事案への対応を行なう組織「シーサート」(CSIRT：Computer Security Incident Response Team)は、今日では多くの企業などにおいて実現されるようになりました。2007年に6つの組織で立ち上げた日本シーサート協議会も、現在では加盟組織が360を超える規模になりました。しかし、一口にシーサートといっても、公的機関、事業者、製造業者、学术界などさまざまな立場の組織があり、その守備範囲も特定のサービスや製品に限定的であったり、逆に組織全体のセキュリティに責任を持っていたりします。さらに、事案対応のやり方も、自組織に高度な技術を持つことで対応に当たっていたり、他の組織と連携する前提であったり、対応手順に特化することで対応の幅を広げていたりするなど、その方針や能力も多様です。

このような状況で、これから新たにシーサートを構築しようとする方とお話をすると、「どこから手をつけたらいいのかかわからない」、「これで十分か自信がない」といった相談を受けることが増えてきました。そこで、シーサートの歴史を簡単に紐解きながら、シーサートにもっとも必要なものは何なのか、考えてみたいと思います。

シーサートの起源は1988年に発生したワームの感染事案にあるとされています。それは、ネットワークに接続された複数のシステムに共通する脆弱性を悪用して感染活動を行なうだけのマルウェアでしたが、一つのシステムに多重に感染することで、処理能力の低下やシステムの停止など、多くの混乱を引き起こしました。この状況に際し、当時のシステム管理者は何が起こっているのか知るすべがなく、多少なりとも状況を知ることができても、その情報を他の組織と共有できませんでした。この経験をもとに、事案に関する情報を一か所に集約して、分析・整理し、その結果を広範に共有することで事案対応を促進する組織として、シーサート「CERT/CC」が米国で設立されました。

シーサートは相互に連携して効果を発揮する機関です。情

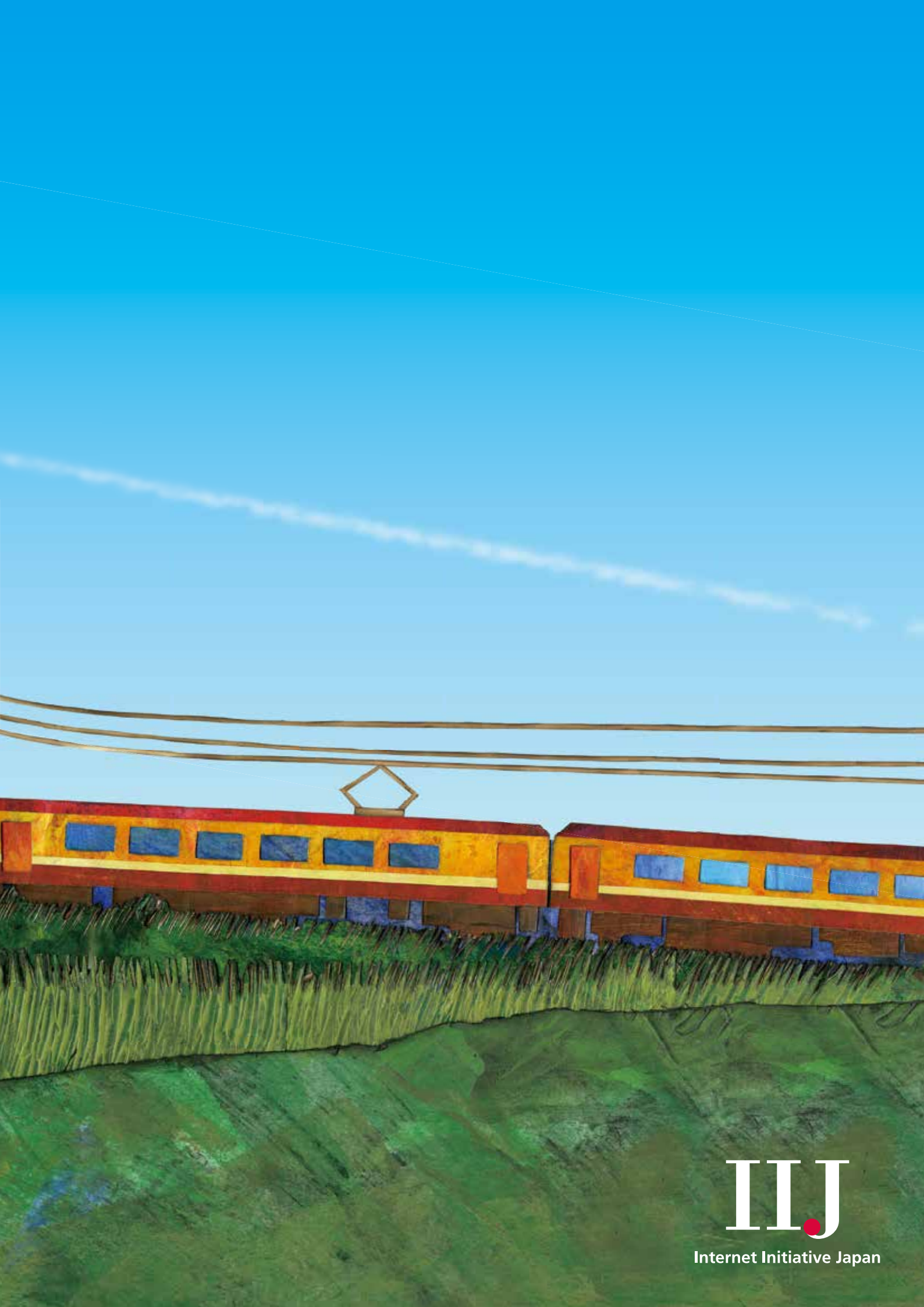


この冊子の内容はサービス形態・価格など予告なしに変更することがあります。(2019年8月作成)  
※ 表示価格には、消費税は含まれておりません。  
※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。  
※ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。  
©Internet Initiative Japan Inc. All rights reserved. IIJ-MKTG001-0153

報を一局に集中し、事案そのものや対応策について情報が流れるようになっても、自分の守備範囲においては自らが対応しなければなりません。また、局所的に発生した事案への対応は、関係する組織間だけで情報を交換することが必要となる場合があり、このような連携のためには、ある程度のルールが必要となります。シーサートの国際団体「FIRST」は、特に国際的な協調が必要な事案への対応の失敗経験をもとに設立されました。たとえ米国と欧州のあいだであっても、夜中にたたき起こされて普段使わない言語でまくしたてられては、そもそも協力しようという気持ちになりません。そのため、言語、タイムゾーン、法制度、技術力、文化、歴史背景などが異なる組織のあいだで連携するために、公用語を英語と定めることや、暗号化通信の使い方など、いくつかのルールが明文化されています。

複数の組織が連携する際には、連携する相手を尊重することが不文律になっており、まずは対応の依頼元が尊重されます。事案の情報を受けたとき、その情報を適切に扱わなかったり、次の組織に渡さなかったりすると、事案対応全体が滞り、不利益を被る人が出るという自覚を持って対応に当たることが求められます。また、対応の依頼先を尊重することも必要です。例えば、自分の国では違法とされる行為であっても、連携相手の国では違法でない場合があり、相手の立場を理解し、対応を強要することなく、連携する必要があるのです。現実には、個別の事案対応にかけられる予算や人員、同時に扱っている他の事案といったシーサート内部の制約により、十分な対応が困難な場合もありますが、多くのシーサートにおいて相手を尊重するよう努められています。

以上のことから、シーサートにもっとも必要なのは、「窓口を用意し、シーサートが機能していると周知すること」であり、そのうえで「連携する相手を尊重しながら対応を進めること」であると言えます。



IIJ

Internet Initiative Japan