サイバー事故現場からの手紙

Letters from Incident Scene vol.1

Table of contents

ラック サイバー救急センターが発行する「サイバー事故現場からの手紙」は、同部門がこれまでに対応してきた事故の実例を踏まえ、インシデントレスポンスに取り組む企業の参考になる情報を提供するものです。このレポートにより事故予防や事故対応の準備が進み、IT の積極的な活用と、事故対応の円滑な遂行が実現されることを祈っています。

1.「サイバー救急」とは何か

日々ニュースで報道される情報セキュリティに関連する事故。個人情報漏えいや機密情報の窃取、脅迫や破壊行為と、被害は深刻化し拡大しているように感じます。
ラックは、2009 年 10 月に、サイバー事件の緊急対応に特化した専門組織「サイバー救急センター」を設立し、業界に先駆けいち早く事故対応のアウトソーシング事業を開始しました。サイバー救急という言葉は、ラックが創った造語ですが、なぜ「救急」という言葉だったのか、その創生の秘密と出動件数 4 ケタという圧倒的な実績の背景にある葛藤や課題について、サイバー救急センター設立以前より、事故対応サービスの必要性を訴えていた最高技術責任者の西本と、現サイバー救急センター長の佐藤に話を聞きました。

広報：年末年始もかなり出動があったようで、忙しい中お二人に時間を作ってもらいありがとうございます。今回発表しましたが、遂にラックのサイバー救急センターの出動件数が 4 ケタ、1000 件[1]を超えたということで、これはものすごい業務の蓄積ですね。

佐藤：私は 3 代目のセンター長[2]ですが、1000 件の事故に立ち会ったというのは、一件ずつの案件の大変さを思い起こすと、大変なことだったなあと、率直に感じますね（笑）
とにかく一件一件が真剣勝負なので、これまで関わっていたすべての案件を思い出すことができます。
これだけ経験すると、お客様のファーストコンタクト[3]である程度深刻さや優先度まで見えてくるんです。

西本：僕はもともとシステム開発からキャリアが始まったんだけど、セキュリティの事故対応って、システム開発プロジェクトでデスマーチ[4]の状況に似てるんだよね（笑）私のキャリアで初めて任された仕事が実は、新入社員一年目だったときに発生したある銀行系プロジェクトの火消しでした。それ以降、私自身もプロジェクトをいくつも炎上させましたが、火消しもしました(笑)

[1] 2006 年の「個人情報 119 番」サービスからの累積件数。
[2] サイバー救急センターのセンター長は、セキュリティ事業トップの丸山などが歴任しているが、実は西本はセンター長になったことはない。
[3] お客様からのお問い合わせの電話を受けること。
[4] IT 業界で言われる、死の行軍と名付けられた困難なプロジェクトをいう。略してデスマ。

広報：お二人ともデスマーチに慣れている[5]ということはよくわかりました。炎上しているプロジェクトというのは、皆関わりたくないというのが当たり前の反応だと思うんですけど、なぜ火中の栗を拾うかのように、「サイバー救急」みたいな仕事を引き受けたんですか？マゾ[6]ですか？

西本：システム開発って、そこにそのシステムを必要としている人がいるっていうのが、仕事のモチベーションですよね。事故の現場っていうのは、まさに我々の力を必要としている方が確実にいらっしゃる場所なんですよね。自分の力を最大に生かせる場があるのって、幸せなことだよね[7]。最初はさ、儲けなんてどうでもよくて、いかにお客様を支えられるか、ってことだけ考えてたよ。良い表現で言うと社会的使命っていうのかな。少し大げさだけどその時は本気[8]でそう思ってたよ。

佐藤：そうですね、その精神は今も受けついでます。我々の部門は、日本でも最大級の陣容で対応していると思う。大型の事故対応案件でも同時に何件も対応できるくらいに充実できました。でもこの仕事で儲けよう、なんて思ったことはない[9]。もちろん損しようなんて思ってないけどね（笑）
お客様から救急コールを頂いて、トリアージ[10]するけれど、コンプライアンスとしては問題はあるんだけど与信も支払の可否も、何も聞かないで対応を始めるんだよね[11]。困ってる人を助けるのって、そういうスピード感[12]じゃないと無理。

広報：えー本当ですか！？[13]

佐藤：めったにそこまでの状況はないけれど、不正送金なんかの犯罪も増えてきているから個人からの質問だってトリアージするからね。

---

5 二人とも、火事場に強いと言われているが、火事場に埋められるという意味でもある。
6 マゾヒストの略。肉体的精神的苦痛を与えられたり、羞恥心や屈辱感を（以下略。反対語はサディスト）
7 仕事人間は家庭を顧みないことがよくわかる一文。
8 今でもそう思っているのがアリアリとわかる。
9 これは本音。実際に対応費用をいただけなかった事例もあったが、さわやかに笑うことで切り抜けられる。
10 作戦会議というべきか、お客様からの情報を分析し、対応の方法を検討すること。
11 ここは読まなかったことにして、意気込みだけご理解ください。
12 意思決定のこと。ワンマンであればあるほど早い。
13 わかってたけれど、形式上の受け答え。

西本：僕の持論は、全ての答えは現場にしかないっていうことなんだよね[14]。研究にしても現場で起こっていることを調べなければ、絵に描いた餅だと思っています。会社の大小や内容の単純複雑ということではなく、いろいろなケースを実際に調べ、それを蓄積することこそが研究なんだと思うんだよね[15]。その結果として発表できたのが、Cyber GRID View vol.1「日本における、標的型サイバー攻撃の事故実態調査レポート」だと思ってます。サイバー救急センターっていうのは、こういう基礎データを得る意味でも重要なんだよね。

広報：今現場で何が発生しているのか、知るために現場に行くっていうことなんですかね。普通の会社じゃこんなことやらないですよね[16]（笑）

佐藤：何事も、最初はこういう漢気[17]がいるってことだと思うね（笑）

広報：実際にサイバー救急の活動を行っていて、企業のセキュリティ対策では何が大きな課題だと思いますか？

西本：最近は現場に行っていないけど、過去から今まで変わりない大きな課題というのは、対策より先に有事の対応の準備をしろ、ってことだろうね。ラックの対策サービスをいくつも提供しているけれど、監視にしても診断にしても、暗号化も ID 管理もセキュリティ対策ってことを行っても事故を完全に防ぐことはできない[18]んだよね。最悪はセキュリティ対策をやったことで安心してしまうことだよね。どんな状況でも事故前提でないのは緊張感のない組織なので、生き抜く上で重要な用心も無くなるからね。
たまにこの話をするんだけど、生きるか死ぬかの戦国時代にいきなり築城するなんてことはないんだよね。今周りで何が起こっているか把握するために斥候を送ったり、見張りを立てたり、攻め込まれることを前提に用心を欠かさなかったわけでさ。

[14] サイバーグリッド構想はここから生まれた。研究と事業を兼ねる社員は、みな疲弊しているとのうわさ。
[15] これまでの対応で得られた固有の情報はすべてデータベースとして蓄積されている。
[16] 別の表現で言うと、当社は普通の会社ではない。
[17] 男ではなく漢。ハンではない。
[18] 言ってはいけない一言だが、誰もがそう思っている一言。

佐藤：そうですよね。家庭だと災害時の避難場所とか、保険に入ったり、水回りならクラシアンのシール[19]とか（笑）そういう有事の対策をしているのに、IT の事故については有事対応の準備をしなくても、撲滅させられるかのように無視していると感じることがあるね。

西本：もう一つ、組織の問題もあるかな。内部犯行をゼロにすることは社長も含めて誰も信じないというように思われがちだけど、そもそも僕は、性善説[20]が全てにおいて機能しないというのは組織として既に終わっていると思うんだよね。高信頼組織[21]を組織の中に有効的にいかに作っていくか、鉄の結束[22]とでも言うのか、そういうものはなくてセキュリティを強化してもね。

広報：事故発生が前提のリカバリーをまずは考えるということですね。実際、それができている会社はありましたか？

佐藤：たくさんありますよ。事故発生を見つけるという視点で、事故が発覚した会社というのはむしろしっかりと対策[23]をしていることが多いんです。逆に事故発生を見込んでいない会社っていうのは、いまだに被害が発生していても気が付いていない[24]のかもしれないね。

広報：そういうことですか。見つけようとしないから事故が発生したかどうかも判明しないと。なんだかすごく腑に落ちました。
この 1000 件の対応で、最も印象に残ったのはなんの件ですか？

佐藤：2008 年の標的型攻撃の調査かな。これは実際に調べてみて、日本でも実は標的型攻撃が行われていたというのが明らかになった、まさにステージが変わった件だったな。

西本：確かにあれは衝撃だったよね。今まで海外で話題になってても日本では現実感が無かった[25]しね。でもさ、今のセキュリティ被害の現状を見ると、あれは幼稚だったなって思うよね。なにせ、今では被害の規模が違う。昔の標的型攻撃なんて、ウイルスちょろっと送られる程度でさ、企業にとってウイルスそのものなんて実際は大したものじゃないんだもん[26]。

19 広告宣伝費用は頂いていません。
20 人間の本性は基本的に善であるとする倫理学・道徳学説。反対は性悪説。「しょうわる」とは読まない。
21 高信頼性組織（High Reliability Organization）のように、事故発生件数を低く抑えている組織、のことではなく信頼関係のこと。
22 ラックでは入社時に行う血の誓いのことを言う（嘘）
23 防御していたので気が付いた、追跡調査のためにデータを残していたという基本的な対策。
24 事故が発生していると想定していないため、ログを見返すことも無く、結果的に気が付かない。
25 標的型攻撃も、インターネットバンキングも、アカウント窃取も、過去から言われていたものが急に現実になった。
26 ウイルスの感染ではなく、そこから意図を持った攻撃が始まることが怖い。

佐藤：そうなんですよね。今の現状でいうと、企業が倒れてしまうほどのインパクトがある被害も想定されるから、とにかく犯人まで到達できるレベルで、事故前提のセキュリティシステムを準備しないと、と思うね。ただ、実際に現場に行くとさ、犯人を見つけ出すどころか、調べる気すらない会社っていうのもある[27]んだよね。証拠を積極的に消してラックが調べても分からないから、事件を闇に葬るという。

西本：これも前から言ってることなんだけど、事故は発生するんだから、発見した事故を見つけた人間は偉い、という認識が広がらないとね。失敗を責めるから、当事者は逃げようとして隠す[28]んだ。もちろんこんな考え方は難しい事なんだけど、事実そうじゃないと事故前提の対策なんてできないもの。

広報：なるほど。失敗を責めると隠す方向に向かってしまうというのは、その通りですね。
ホント、このお話をしだすと朝までかかりそう[29]です。
さあ、これまでの 1000 件を踏まえて、これからのサイバー救急センターはどこに向かうのでしょう？

佐藤：そんなに晴れやかな未来が待っているとは思えないんですよね[30]（笑）
正直、今のサイバー救急センターは、チームのメンバーのモチベーションというか、使命感だけで乗り越えている感じなんですよね。家に居ても買い物をしていても、事故が発生したらいつでも出動[31]することになる。リーダーとして今の状況で耐え続けてくれとは言えないんだけれど、事故は日々発生している。今年は、我々のパッションだけで乗り越える今の仕組みから、もう少し先に進めたいと思ってます。調査の自動化も、今回のレポートのようにお客様の事故対応の啓発も、メンバーの育成も。
そして戦いの場でも息抜きができる楽しい職場、そういうものも実現したいと思ってます。こういったバラ

---

27 調査しています、という事実が重要で、根本的な問題に目がいかない。
28 正直に話すのが偉いというのは、ワシントンと桜の木の話が有名。
29 いつも飲み会ではこのような話が長くなり帰れなくなることをさしている。
30 身もふたもない。
31 突然仕事に戻る夫や彼が、家族や彼女に責められ葛藤するシーンがドラマでありますが、こちらはリアル。

ンスを大切しないと、次の 1 万件[32]の出動は対応できないですからね。

広報：チームを大切にする佐藤さんらしい抱負ですね！常に緊張を強いられるだけでは、生身の人間は耐えられないですもんね。
西本さん、自分が立ち上げたサイバー救急センター[33]ですが、企業の経営者の視点から、どのようない期待をしていますか？

西本：正直、今のサイバー救急センターは、業界でも最高クラスの体制と経験があるから、何も心配していないんですよね。でも、実際に事故に見舞われるお客様には危機感を感じるかな。特に地方[34]だね。
僕が豊彦[35]にお願いしているのは、サイバー救急センターのノウハウをどんどん共有・公開して、地方の現場で対応できるような仕組みを作りたい、ということです。言ってみれば、地域の青年団とか消防団みたいな感じかな。勉強会をしたり、自分らでピンチを乗り越える方法をお伝えしたい。これがサイバー救急の究極の在り方[36]なんだと思う。
これからもサイバー救急センターには、経営者として、セキュリティ業界人として期待しています。

広報：いつの間にか政治家みたいな話し方[37]になってますね。事故対応はセキュリティ対策の第一歩というお二人のお話を聞きながら、次の 5 ケタの出動がずっと来なければよいのに[38]、と思います。

32 大きく出ました。
33 センター長になったことはありません。
34 情報流通、支援体制が課題と言われている。
35 佐藤は社内で下の名前で呼ばれている。広報は最初、豊彦という名字だと思っていた。
36 特別な資格などが無くても、スキルや支援体制があれば IT の救急は行える。という意味。
37 国や業界といった、マスを意識した発言を指している。
38 サイバー救急が忙しいということは、IT にとっては歓迎すべきことではありません。

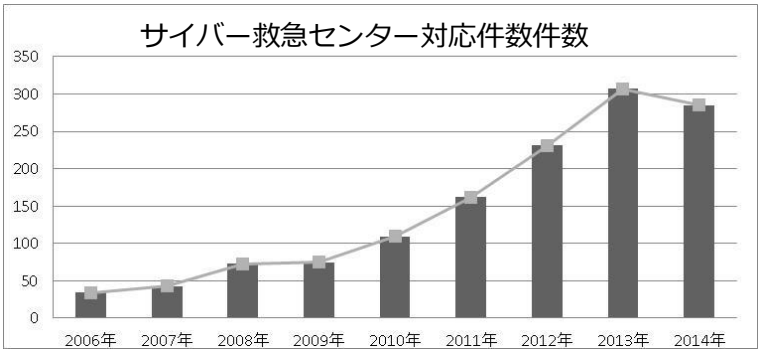
2. サイバー救急センター9 年の歴史

サイバー救急センターは、2009 年 10 月に正式に組織化され、発足しました。しかしラックとして事故対応の支援を始めたのは、2006 年の「個人情報 119 番」サービス提供開始までさかのぼり、事故対応サービスの歴史は 9 年になります。

サイバー攻撃による被害を、社外の組織に知らせて支援を求めるというのは、その当時はタブーとされていたなか、当社は今後、セキュリティインシデントが頻発し、被害も増大することを予測しての組織化となりました。

しかし、サイバー救急センター開所当時は十分な組織体力もなく、経験も十分とは言えませんでした。今の下地となるインシデントマネジメント、フォレンジックといった機能が拡充し、複数の案件を同時に対応できるようになったのは、2011 年のことです。

この年から、それまでしばしば救援要請をお断りしなければならない脆弱な体制であったものを、重大事案はすべて対応可能な体制に強化し、その後の 4 年で 1000 件を超える出動実績を記録することとなりました。



右の図にあるように、直近 4 年間の対応件数が 1000 件を超えたことをうけ、サイバー救急センターのこれまでの取り組みを振り返り、統計情報からみる傾向分析を掲載します。

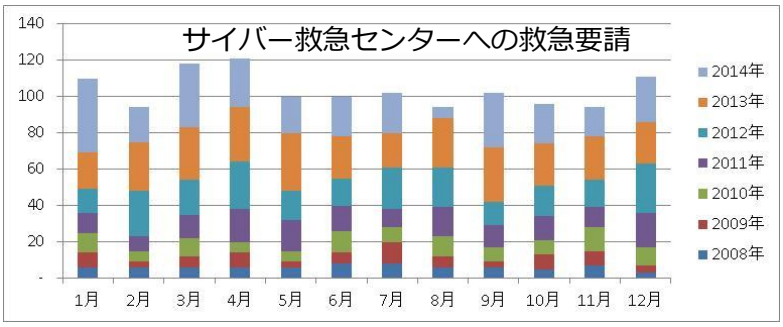
1. 救急要請があった時期の傾向について

先のグラフで明らかなように、サイバー救急センターへの救急要請のペースは急拡大しており、後で取り上げますが被害の深刻さも増しています。一年に 300 件の出動ペースは、ほぼ一日に 1 件発生していることになり、出動に至らない電話での相談も含めると、一日に数件の問い合わせが入っていることになります。

かつてはサイバー事件での被害を、社外に情報を提供して問題解決に当たることは一般的ではありませんでしたが、昨今の複雑かつ巧妙な犯罪行為と、被害の深刻さにより、専門知識をもつ当社への問い合わせが加速しているといえます。

なお、この対応件数の中には、当社のセキュリティ監視センター「JSOC」での被害検知を発端とした案件も含まれており、セキュリティ機器の性能向上による「気付き」の機会が増えたことも一因となっています。

月別での問い合わせ傾向からは、明確な傾向はみられませんでした。

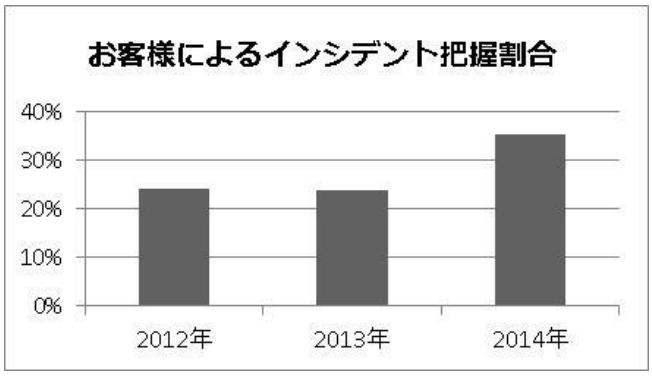


各年で大きく傾向が変化しており、2 月と 8 月に経済活動が鈍化する、いわゆるニッパチの影響も軽微です。しかし、セキュリティ診断や年度の切り替わりに行われる IT の保守点検などのタイミングで、セキュリティインシデントの発見が増加する傾向はみられ、仮に一年を通じてサイバー攻撃が行われているのであれば、毎年 5 月から 11 月に一度、情報漏えいチェックサービスなどの被害有無の確認を行うことも有効です。

2.　重大案件の増加について

サイバー救急センターでは、実際に現場で原因究明を含めた作業を行い、深刻な被害が確認されたケースを、重大案件と定義しています。お客様も当社も、多大なリソースを投じて問題解決に当たらなければならないようなケースが増えており、企業の深部へ侵攻し情報を窃取し、破壊活動をするような攻撃による被害が拡大しています。

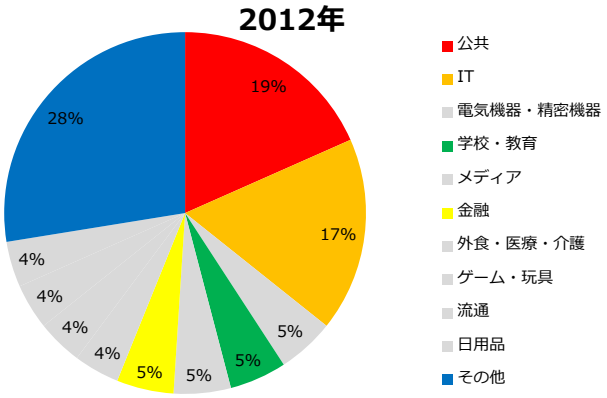
重大案件の特徴としては、攻撃活動は周到に行われており、ウイルス対策ソフトや単純な検知機器だけでは被害を発見することはできません。昨今の複数の高性能な検知機器や CSIRT 組織の設置、何より「自社も被害にあっているかもしれない」という危機意識により、発見の頻度が高まっていることが案件数の増加につながっていると考えています。



また、以前はサイバー救急セン

ターへの支援要請があったケースでは、お客様側では何が発生しているか分からない状態でありましたが、最近では、先に説明したようにお客様自身による一次調査が済んでいるケースもあり、この場合にはラックに原因追究や説明責任を果たすための報告書作成の意図があると考えています。

しかしながら、当社に連絡を頂く前に、被害にあわれたかた自身が独自の調査を行うことで、証拠を消してしまうケースが散見されます。たとえば、ウイルス対策ソフトによる駆除や、動作ログの削除などがこれにあたり、この場合最終的な原因追究に支障が出ることがあります。これらのことを考えると、発見時のスムーズな調査、専門組織へのエスカレーションルールなどの規定の制定が必要となりそうです。



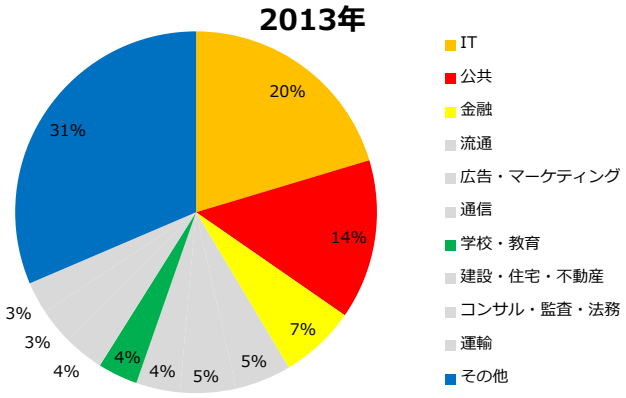
支援要請業種別割合

3. サイバー救急センターへ連絡いただいた組織の業種について

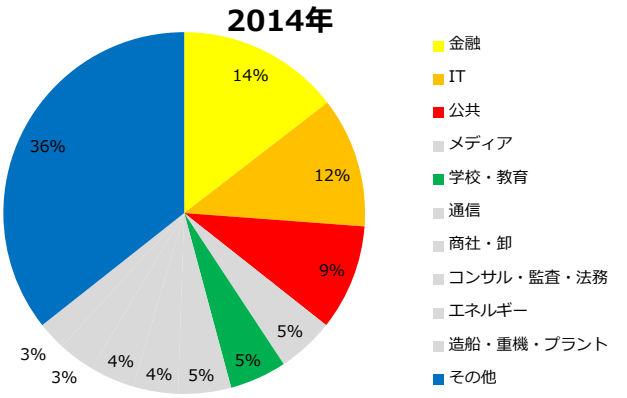
一般に、サイバー攻撃を受ける企業は、個人情報や機密情報など機微情報を持ち、クレジットカードやその他金銭に関わる情報を持っている企業、と考えられがちですが、その傾向は少し変化し始めています。

当社へ支援要請している企業の統計情報ですので、実際にすべての企業の状況を正確に網羅しているわけではありませんが、常に被害を受ける上位にあるのが、公共組織、IT 関連企業、金融、そして大学など教育現場です。

これらの業種は、攻撃の対象になりやすい要素があることを認識し、攻撃を検知する能力を実装いただきたいと思います。



支援要請業種別割合



支援要請業種別割合

また、グラフの青、「その他」の割合が増えていることから、攻撃対象の業種が拡散し、それぞれに標的を散らばらせた攻撃に移行している可能性があります。
これまで攻撃が少ないと考えられた業種であっても、攻撃対象になるかもしれない、という意識を持っていただきたいと思います。

なお、攻撃を受けた上位 5 業種で被害件数の約 5 割、上位 10 業種で 7 割ほどを占める状況です。これを見ると攻撃対象が偏っていると捉えられますが、ある企業の被害が表ざたとなり、同業の他社も調査をして判明したケースもありますので、単に攻撃対象が偏っている、とは言い切れません。

4. インシデントの再発割合について

サイバー救急センターに支援要請があり、被害の把握と復旧作業を行った後に再度インシデントが発生した企業は、下の表のように確実に増加しています。

2012年	2013年	2014年
8%	21%	28%

サイバー攻撃の被害が再発する理由はいくつか考えられます。

- その企業が攻撃者にとって非常に重要な情報などを持っている
- 攻撃対象に特化したマルウェアは、既存のウイルス対策ソリューションでは見つけにくい
- 事故対応後 JSOC など監視サービスを導入し、出口対策で食い止めたイベントから判明する

昨今のサイバー攻撃は、執拗で巧妙な手段を使って企業のシステムに入り込みます。企業は、攻撃を未然に防ぐことも重要ですが、如何に攻撃による被害が発生した時に素早く認知できるように準備するかが重要であり、このイベント再発割合の増加は、セキュリティ対策が継続して有効に働いていることの裏返しです。
逆に言うと、これまで一度も被害を発見できていない企業は、被害が発生していないのではなく見つけられていない可能性があることを念頭に、情報漏えいチェックサービス等での現状把握をお勧めします。

5. インシデントの原因・手段（2014 年）

セキュリティインシデントで最も注目されるものが、どのような攻撃手法・手段が用いられ、どのような被害が発生したかというものです。

当社が対応した重大案件において、下の表のような攻撃手法・手段により被害が発生したことが確認されています。これは攻撃の取っ掛かりを割合として示したもので、実際には企業内に侵入を許してから、これらの手法を複合的に用いられ、情報の窃取や遠隔操作可能なインフラ構築が行われます。

外部からの不正侵入	標的型・APT（侵入）	ID の不正利用	USB 等の不正持出し	マルウェア	その他
35%	13%	12%	3%	29%	9%

ネットワークを経由した不正侵入や、一般に使われているマルウェアの悪用が多くの割合を占め、標的型攻撃については 1 割強となっています。しかし、標的型攻撃の場合には、攻撃を受けた企業が被害に気が付いていない可能性があり、この割合については参考的なものとしてとらえていただいた方が良いでしょう。

また、下の表は発生した被害の分類を示しています。幸いにして機器やデータの破壊を伴うものはありませんでしたが、マルウェアの感染被害が広がり、社内のデータの漏えいや内容の改ざん(主に Web サイト)といった被害が出ています。その他被害の中には、金銭の不正送金や管理者権限の奪取などが含まれています。

改ざん	漏えい	破壊	不正使用	マルウェア感染	その他
15%	25%	0%	16%	32%	13%

まとめ

サイバー救急センターが対応した 1000 件を超えるインシデントレスポンスと、数百件に及ぶ重大案件から、皆様が CSIRT 組織を保持し、事故対応の準備を進めていただく認識をお持ちいただける材料が提供できたのではないかと思います。

攻撃者の巧妙さを考えると、インシデントが発生することは、もはや恥ずかしい事ではありません。もし不測の事態が発生した場合には、「サイバー救急センター」までご連絡ください。

3.「保全活動」における 5 つの事例

不正アクセスなどのサイバー攻撃が発覚した時に、協力要請を受けるのがフォレンジック調査（デジタル・フォレンジック）です。フォレンジック調査をすることで、サイバー攻撃による被害の影響範囲や深刻さ、そしてサイバー攻撃を受けてしまった原因となるものを解明します。フォレンジック調査で重要なものが調査対象機器の「保全」作業です。保全作業はその調査対象機器の状態をそのまま証拠として調査分析に用いるため、とても重要な作業工程と言えます。
ラックはこれまで数百件に及ぶ事故対応を行う中で、数多くの保全作業（ディスクイメージの複製）をしており、これら事例から、きっと参考になる内容をまとめます。

1. 保全データ数、データ量が多い（保全対象が数 TB あり、保全作業を数日要した話）

ここ最近は、保全対象機器の物理 HDD サイズが拡大する傾向にあるという事を懸念しています。そして、発生するインシデントによっては保全対象の対象機器が数十台になるケースがあることも増えています。保全作業を行うという事は、もちろん調査を行うから証拠保全を行うという図式です。数が多いと調査担当にも労力をかけますが、その前段階である保全作業も保全担当からするとかなりの労力を必要とします。
ここ最近のサーバの物理 HDD ディスク量は数百 GB を超えるものが増えています。保全作業においては専用機器を使用する場合と、専用ツールを使用する場合があります。どちらの場合も大体 1GB のデータ複製、転送に約 1 分程度の時間を費やすこととなり、保全作業の実作業時間は物理 HDD ディスク量に比例して増大します。もちろん、マシンが停止している状態、もしくは動作している状態によっても作業時間は変化します。
以前、サーバ十数台の保全作業を行った際、サーバの設置場所は関東圏内外の数ヶ所に分散設置され、対象物に NAS として利用しているサーバも含まれており、データ領域が 1TB のものもあるような状態でした。しかもお客様のご意向でサーバ停止が行えないという状況でした。このように保全作業が長時間になることが予測され、遠隔地の場合なども、基本的にはお客様自身での保全作業を実施するよう依頼します。ラックのエンジニアが長時間の作業を行うことで費用も高くなりますし、お客様の都合の良いタイミングでの作業が可能となるためです。しかし、あるお客様のケースでは、ラック社員が全ての拠点へ出向き保全作業を実施することになりました。これはお客様からの強い要望によるものでした。
この時は、なんと 1 サーバあたり約 7 日～10 日の保全時間を費やすことになり、お客

様、ラック共にかなりの消耗をしました。
記憶装置の大容量化は、ビッグデータの保存に必要となっていることは理解していますが、フォレンジックにおいては、非常に厄介な時代になったと感じています。

2. 保全対象がクラウド上のサーバだった

ここ最近の問合せで多くなってきたのが、ISP や通信業者が提供するクラウド上のサーバにおけるインシデントの相談です。サービスを提供する事業者との契約体系は多種多様ですが、ここでは VPS/クラウドホスティングなど OS の管理者権限を与えられ、コマンドやカスタマイズも自由に利用できるサービスを取り上げたいと思います。
昨今、この種のサービス事業者が急拡大し、価格競争の影響からか月額費用が低価格で押さえられていることが、利用者数が増加することに拍車をかけ、その結果ラックへの事故の相談が多くなっている理由となっています。
自社でプライベートクラウドを構築している企業であれば、クラウドサーバの保全作業はスムーズに行えます。しかし事業者が提供してサービスの場合はデータの保全で問題となることが多く発生します。
保全作業においては、クラウドサーバのハードディスクイメージ取得をすることになります。通常のサーバだと USB-HDD などを物理機器へ接続し、専用ツールにてイメージを収集するのですが、クラウドサーバの場合、基本的にそれが行えません。事業者所有の設備であり、そして運営システムであるため、設備への立ち入りも機器の操作も基本的に認められません。クラウドサービスの利用契約でも、データのイメージ取得は認められていない現状です。
そうなると、物理的なサーバを目の前にしての保全作業は無理であり、ネットワーク経由でディスクイメージを収集する方法しかありません。クラウドサーバの保全作業はネットワーク経由であるため、作業時間は通常の保全作業と比べ極めて遅くなります。もちろん、データ転送中は事業者側の回線帯域を消費することになります。
事業者によっては回線帯域の消費により、データ転送中の通信を止めるなどの処置を講じられる場合もあるので、保全作業は注意が必要となります。
クラウドサービス事業者がデータ保全のための帯域消費を許容せず、通信を止められたという問題も発生することがあり、注意が必要です。
クラウドサーバの保全をする場合、管理者権限でのコマンド操作が必要なため、それが許可されないクラウドサービスは残念ながらフォレンジックの対応するのが困難であるというのが実情なのです。これは ASP サービスにおいても同様です。

低価格やデータ容量、使い始めるハードルが低いなど多くのクラウドサービスがありますが、事故が発生した時のリカバリーについても気を付けて選択することをお勧めします。

3. 関係者による証拠隠ぺい

これは言いにくいことですが、お客様が調査の結果を恐れ証拠となるデータを消してしまうケースがあります。
あるケースでは、個人所有の PC のフォレンジックを試みようとしたところ、見られたくない情報があったためか、HDD の WIPE、再インストールの処置を講じた後でした。
オフィスへ個人所有 PC の持込み、もしくは USB メモリを介して業務 PC にマルウェアが感染するなどのインシデントは、ラックの調査においても少なからず存在します。その場合、そのインシデント発見起因は業務 PC の動作が重くなったとか、不審な通信を確認したといった、原因を調査しなければ分からないものです。ほとんどのケースは業務 PC 上にインストールされているウイルス対策ソフトが警告を発しません。

業務 PC のマルウェア感染を調査して行くうちに、感染の経路として使用された物理媒体等が判明する場合があります。また、さらなる感染経路を調査する企業も増えており、その場合は企業が個人所有 PC に対しての調査を依頼される場合があります。それは、業務 PC が本当に個人所有 PC から感染したのか、という裏付けの調査です。
個人の PC である故、音楽データ、画像や個人所有の情報が盛りだくさんであり、その方の立場では、第三者に見られたくない情報もあることでしょう。そのため、自分の行動などを証拠として残さないため、個人が PC をフォーマットや工場出荷状態にする処置を講じる場合があります。当社としても保全作業を行い調査を試みますが、このようなケースでは完全な調査が成功することはほとんどありません。
この場合、個人が明確な意図（証拠の削除）をもって行動しているので仕方がありませんが、調査対象機器の状態をそのまま証拠とし調査を行うためには、そのままの状態を保ち保全を行うことが重要です。データ削除につながる操作や作業については十分に注意していただきたいと思います。
また、企業のご担当者には、個人所有の PC への調査に踏み出す場合は、十分に個人への配慮、十分な説明、調整を行うことが必要となりますので、こちらもご考慮ください。

4. 拠点ご担当者への情報共有

これは、サイバー救急の要請をされたお客様内のコミュニケーションの課題です。
本社の依頼で地方拠点にて保全作業を試みようしたところ、地方拠点の方々から、「何が起きたの？」などの質問を頂くことがあります。地方拠点には作業者が行く事だけを伝えただけで、詳細な情報は伝えてないケースでは、必ず起こる問題です。
通常、地方拠点側の保全作業は、地方拠点側の担当者と話をして保全作業を進めます。しかし、まれにあるのがコマンド実行などは全て本社側からリモート環境で行い、保全作業を実施するやり方です。このような手法をとるのは、地方拠点側にシステム担当が居ない場合です。このケースでの我々の作業は、単にディスクイメージの保存先として持ってきた USB-HDD を差し込み、データの保全が行われたら抜き取る、という作業です。しかしこの作業であっても、お客様の手を煩わせて立ち会っていただきます。
地方拠点側の立会いの方は、なぜ作業をするのかも本社から知らされておらず、作業者へ「何かあったの？」、「どんな作業しているの？」、「どれぐらい時間かかるの？」、「何時まで作業立会をしなくてはならないの？」、「本社で何あったの？」などなどの質問を頂くことになります。
全てを地方拠点の方に説明できないことは理解できますが、本社の方々は地方拠点の方へある程度の情報伝達をするなど、重要で深刻な状態だからこそコミュニケーションをしっかりとり、よく対処していただきたいと思います。
深刻なセキュリティインシデントであるため、社内向けに開示できないというのは理解できますが、その場合であっても「保守作業があるので、サーバ作業が行われるから協力してあげてほしい」とだけでも伝えていただけるとスムーズに作業が進みます。

5.　保全作業の環境・手順などの過酷さ

これは、コンピュータとか、ネットワークといった話ではなく、作業員である我々の肉体や精神への負担のお話です。
私たちは、お客様からの支援要請によりトリアージをし、重大な事案の場合には原因追究のために証拠保全を行うため、お客様サイトへ訪問します。この作業は非常に重要であり、早急かつ確実に行わなければなりません。しかし、保全作業は簡単に実施することができません。
データセンターでの作業は厳しい環境であることが多く、まずはデータセンターへ入館することができない場合があります。入館できてもサーバルームが極寒で、夏に防寒着

を持たない状態で何時間もサーバルームでの作業を行い、風邪をひくこともあります。
また、簡単にサーバルームから出られない施設もあり、行動が制限されます。
データセンターの設備の把握や契約内容の把握、入館連絡の方法など事故対応の緊急時に向けて事前の準備をお願いしたいものです。

また、お客様から支援要請があり、オンサイトを実施すると決まった時にはもう夜で、現地に向かうと帰りの電車が無い場合もあります。電車が無いだけではなく、データセンターは繁華街から遠い場合もあり、この場合にはタクシーを捕まえることも難しくなります。地方では深夜のタクシーが探せない場合もあるなど、交通手段の問題はわりと深刻な場合があります。

最も厳しいのは、保全作業が複数の拠点で行わなければならなかったり、一度に複数の異なる事案が発生しまさに保全作業のハシゴになる場合があり、肉体的・精神的に追い込まれることがあります。これは当社のように体制が充実していても過密状態は発生しますので、一時的な波を乗り越えられる強い精神を養わなければなりません。

さいごに

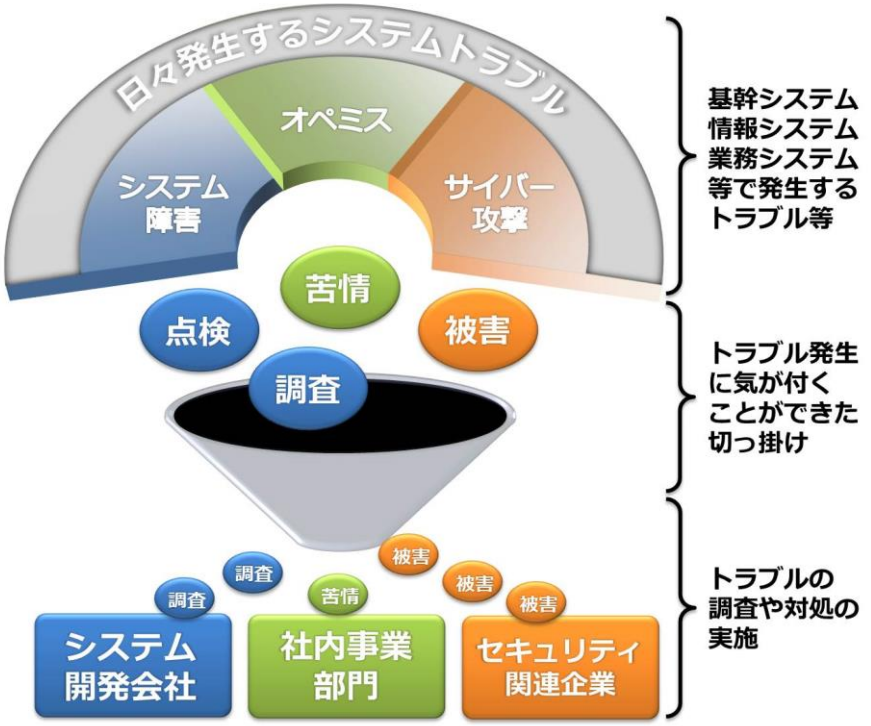
ここに挙げた 5 つの事例について、この内容がそのままお客様の活きた知識になるとは思っていませんが、もし事故が発生した時に、データを保全して調べる際のコツとしてご理解いただければと思います。
私たちサイバー救急センターは、お客様が原因を知りたいという思いがあれば、出来る限りの協力をさせていただきたいと思います。

4. サイバー事件簿：故障だと思ったら…

サイバー救急センターは、コンピュータシステムが何らかの事件・事故に見舞われ、原因調査や復旧などの支援が必要な企業に対して、初動から問題の解決までの一連の活動をサポートする部門です。サイバー救急センターには、毎日 1 件以上の支援要請が寄せられますが、今回は重要な指摘を含んだ事例について、同センター　インシデントマネジメントグループの関グループリーダに話をききました。

セキュリティレスポンスで最も重要なことは、当たり前ですが、攻撃されていることを知ることです。しかし多くの場合、被害企業が攻撃されていることが発見できないよう、水面下でコソコソと活動しています。

サイバー攻撃の調査の取っ付きは、ほとんどの場合、日々システムで発生しているトラブルの調査から始まります。発生しているトラブルを把握せず、その内容を精査しなければ、残念ながらインシデントレスポンスのスタートは切ることができません。



ある中堅企業がいかにして攻撃の事実を認知し、対応を進めたのかをまとめます。

この事案の対応が始まったのは、まだセキュリティインシデントでもなんでもない単なるサーバトラブルに関する問い合わせでした。
切っ掛けは、「ここ数日サーバの動作が変だ」という相談が当社のエンジニアに届いたことから始まります。メッセージを送ってきた方は当社のエンジニアの知人で、システムの不調の原因調査の方法について相談してきたのです。
不調の表向きの症状は、突然通信ができなくなったり、サーバのリソースが減りレスポンスが遅くなるといったものです。当社のエンジニアは、一般的なパフォーマンスチューニングや問題特定の方法を紹介し、どのような通信が行われているのかも含めてデータを取ることを勧めました。

この段階では、誰もこの問題を大きく捉えておらず、一般的なシステムトラブルだと判断していました。しかし後日その担当者から当社のエンジニアに連絡があった時、状況は少し変わっていました。
サーバのパフォーマンスログでは不審な状況は判断できませんでしたが、通信の内容に気になる情報があるということで、正式な調査要請を受け、サイバー救急センターへエスカレーションされました。

連絡を受けたサイバー救急センターでは、状況のヒアリングから収集されたデータを分析し、確認された通信データが、その会社の事業関連の情報であることを即座に把握できました。至急応急処置としてマルウェア対策機器の一時的な利用による保護と、脆弱性を発見するセキュリティ診断を実施しながらも、流入経路や被害状況の把握を勧めました。
そうしたところ、その会社向けにカスタマイズされたマルウェアの存在が確認され、そのマルウェアは数か月前から社内に潜伏していたことが分かりました。複数のサーバやクライアントに対してマルウェアの感染が確認され、問題の大きさが発覚しました。
この時点で情報システム関連部門だけではなく、グループ企業や関連企業への影響も想定され、社内の対策チームが組織されました。
恒久的な対策のため、それまで活用していたデータセンターを変更したり、グループ企業全体の情報漏えいチェックを行うなど徹底した被害の把握を行いました。
この作業が完了したことで、ウイルス感染およびデータ窃取の範囲がおおむね把握でき、それに伴い再発防止策を検討する流れにつながりました。

この事案の教訓は、当初のシステムの不調を見過ごしていたら、このようなセキュリティの問題として認知することもなく、今なお情報が窃取されている状況であったということです。システムマネジメントがしっかりと行われ、問題の分析を丁寧に行っていたからこそ発見できた事案で、大きな被害につながらなかったことは不幸中の幸いでした。私たちが対応した他のケースでは、グーグルのセーフブラウジングで企業 Web が不正と判断されたが、実際のコンテンツは何も問題が無いというケースがあり、グーグルのミスだと思ったが、根気よく調べると何とウイルスがコンテンツを書き換えたり戻したりを繰り返していた事案がありました。いつもと何かが違うと感じたら、しっかり原因を調べつくすという姿勢が必要です。

サイバー救急センターには、年間 300 件以上の事故対応を行っています。
この状況を考えると、平常なシステムの運用状況を的確に評価したうえで、たとえ小さな問題であっても見過ごさずに調査を行い、状況により第 3 者の支援も受けながらオペレーションマネジメントすべきと考えています。

株式会社ラック

TEL: 03-6757-0113　E-MAIL: sales@lac.co.jp

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

http://www.lac.co.jp