# 医療機関を標的としたサイバー攻撃にどう対処すべきかを考える

アメリカ大統領選挙の期間中、ロシアがアメリカにサイバー攻撃を仕掛けたことが明らかになり、世界中の注目を集めている。こうした時代にあって、患者データやカルテの医療情報など、漏洩が許されない情報を集積している医療機関は、大きなリスクを抱えていると言っていい。インターネットに接続したPCがどこにでも存在する医療現場は、まさに危険と隣り合わせである。それに対し、医療界はどう対処していったらいいのだろうか。1月25日の当会では、サイバーセキュリティ技術者の中でも圧倒的な知識と技術を持ち、世界中の各国政府から「トップガン」の異名を取る名和利男氏に講演頂いた。

## 国もサイバー攻撃対策に力を入れ始めている

当会国会議員団代表の原田義昭・自民党衆議院議員から次のような挨拶があった。

「日本の医療と医薬品等の未来を考える会」国会議員団会長
自民党衆議院議員
**原田義昭氏**

「サイバー攻撃に対するセキュリティ対策は、国の安全・安心にとっても重要な問題です。医療界にとっても、非常に大きな影響をもたらすのではないかと思います。データのデジタル化が進んだことで、危険も増しているといえます。重要な個人情報ですから、漏洩するようなことがあれば大変なことになります。現状がいかに進んでいるのかを知り、常にフォローしていく必要があるようです」

自民党衆議院議員、医師
**冨岡 勉氏**

また、冨岡勉・自民党衆議院議員（医師）からは、次のような挨拶があった。

「サイバーセキュリティが重要ということで、政府も人材育成に取り組んでいます。私は昨年8月まで文部科学副大臣として、情報処理安全確保支援士という国家資格を作ることに取り組んできました。今年4月に第1回の試験が行われます」



講演採録

## サイバー攻撃に対処するためのプログラムを構築しておく

サイバーディフェンス研究所
専務理事・上級分析官
**名和利男氏**

「サイバー空間における『攻撃側』の背景及び行動を直視する』という題で、サイバー攻撃における攻撃者についてお話します。サイバー攻撃の攻撃者は、現在はまだ人間です。それがどのような素性の人間なのか、それに対して、防御側の私たちの実態はどのようなものなのか、ということについて知っておくことは重要です。

まず理解しておいていただきたいのは、攻撃側と防御側のレベルの差です。攻撃側の能力は「エベレストに登頂できるレベル」です。それに相当する技術力と知力を持っています。対する防御側の能力は、「幼稚園の砂場に作られた高さ13㎝の砂山に登れるレベル」です。そのくらいの差があり、さらに広がっていくと考えられます。従って、必ずやられてしまうと考えておく必要があります。

また、欧米各国には異なる人種、文化、宗教が存在し、そこで構築される内部ネットワークは基本的にお互いを信じません。ところが、日本ではお互いを無条件に信じてしまう文化背景があり、内部ネットワークもそのように構築されています。これだと、サイバー攻撃を受けた時に、瞬く間に全部がやられてしまいます。

これまでにも世界では多くのサイバー攻撃が行われてきました。冷戦時代における旧ソ連のパイプライン爆破事案、1999年のユーゴスラビア紛争、2001年の海南島事件、03～09年の西側諸国の国や企業に対する大規模攻撃、07年のエストニアやシリアにおけるサイバー攻撃、11年の韓国農協銀行事件、10～14年の日中間の歴史認識の差が拡大して生じた918攻撃、15年のイスラム過激派組織によるサイバー攻撃などです。

誰がサイバー攻撃を行っているのかというと、現在では国家が中心になっています。そうしたこともあって、攻撃能力は非常に向上しており、相手国を潰しかねないほどになっています。

また、現在の攻撃者は、自ら手を下さないことが多くなっています。ハッキング技術も持っていません。国家が攻撃を仕掛ける場合には、国の役人や軍のトップが攻撃者です。マフィアが金を得るためにサイバー攻撃を仕掛けることもありますが、その場合はマフィアのトップが攻撃者です。彼らは自ら手を下すのではなく、サイバー攻撃の専門家にやらせるのです。

では、サイバー攻撃にどう対処したらよいのでしょうか。「サイバー攻撃対処プロセス」を構築しておくことが大切なのですが、その時に参考になるのが、人間の危険回避のための行動です。例えば、私が水の入ったペットボトルを人がいるところに投げ付けたとします。そこにいた人たちは、目や耳などの感覚器官でそれを感知し、情報を脳に伝達します。脳は私がやろうとしていることを瞬時に理解し、ペットボトルがどういう放物線を描くかを計算し、当たらないための回避行動をとります。脳から筋肉繊維に情報が送られ、手足を動かしてペットボトルをよけるのです。この「認知－判断－動作」という危険回避のためのプロセスを参考にして、サイバー攻撃に対処するプロセスを構築しておくことを勧めます。

伝達された情報を元に判断する脳に相当するのは、経営層の人や組織のセキュリティ担当者です。この人たちが、現場から上がってくる情報をよく理解できるのかがとても重要です。また、その判断に従って出された指示に従い、確実に対処していく必要があります。そこに外部の専門業者が必要になる場合もあります。

さらに、サイバー攻撃対処の行動を、演習・訓練しておくことも極めて重要です。

## サイバー攻撃対策について突っ込んだ質疑応答が展開

講演後に質疑応答の時間が設けられた。出席したメンバーにより、次のような議論が行われた。

**尾尻佳津典・「日本の医療と医薬品等の未来を考える会」代表**　「攻撃側はエベレスト登頂レベル、防御側は幼稚園の砂山レベルだとすると、政府の情報でも、病院の情報でも、盗もうと思えば盗めるということですか」

**名和利男**　「そうです。やろうとすれば必ず出来ます。ただ、すぐ出来るのか、半年後なのか、2年後なのか、という差はあります。そして、病院のデータが盗まれていても、攻撃側がミスをしなければ、盗まれている側はそのことにまず気付きません」

**荏原太・高田中央病院院長**　「小さな病院で電子カルテを使っています。情報漏洩のことを考えると、データを1カ所に集め、政府の管轄で守った方がいいのではないかと思いますが、いかがでしょうか」

**名和**　「現在は、そういった方法が最善の策であるとして推奨されています。例えば、サイバー攻撃対策に1000万円を使うとして、ここにある20台ほどのPCそれぞれに対策を施すと、1台当たり50万円を切ってしまいます。データを1カ所に集めて対策すれば、そこに集中してお金を使うことが出来ます。サイバー攻撃対策のコストには限度があるので、その中で最大の効果を引き出すことを考える必要があります。ただ、電子カルテの情報を1カ所に集めるべきかどうかについては、それだけで判断することは出来ませんが」

医療法人すこやか
高田中央病院院長
**荏原 太氏**

**大津信弘・帝京大学本部情報センター特命課長**　「システム的に情報漏洩を防ぐことは無理だと判断し、早期発見、早期対策に主眼を置いています。現在は、オンラインでもオフラインでも守り切れないとのことですが、どういうところに注意するのがよいのでしょうか」

「日本の医療と医薬品等の未来を考える会」代表
集中出版株式会社代表
**尾尻佳津典**

帝京大学本部情報センター
特命課長
**大津信弘氏**

**名和**　「2016年3月から急激に多くなっているのは、コンピュータウイルスやマルウェアを使わない攻撃です。ただ、17年1月からは、またがらりと攻撃の仕方が変わってきました。このようにサイバー攻撃はダイナミックに変化しているので、それを知って対応をとる必要があります。いたちごっこですが、それが重要なのです」

**大津**　「そうなると、継続して専門的なコンサルを受けていないと、対応しきれないですね」

**名和**　「その通りだと思います。文部科学省が人材育成に力を入れています。専門的な知識を身に付けた国家資格を持つ人材を雇って頂くのがいいのかな、と思います」

**弓信幸・厚生労働省参事官（サイバーセキュリティ・情報システム管理担当）**　「政府としましても、医療機関は重要インフラということで、サイバーセキュリティに取り組んでいこうと進めているところです。医療分野において、今後想定される攻撃の特徴を教えてください」

**名和**　「インターネットを通じて医療機器をコントロールし、あるいはセンサーとして利用し、さらにはそれを連携させるという攻撃が始まっています。先日、ある病院で、患者の命には関わらなかったのですが、医療機器がサイバー攻撃を受けてしまいました。インターネットを活用する医療機器はリスクがあるかな、と思います」

厚生労働省参事官（サイバーセキュリティ・情報システム管理担当）
**弓 信幸氏**

**荏原**　「サイバー攻撃でお金を取るランサムウェア（身代金要求型不正プログラム）による攻撃は、医療関係では起こり得ないのですか」

**名和**　「アメリカでは既に起きています。日本の医療機関では、経理を行っている人のネットワークと、医療現場のネットワークは完全に分離されていますから、入り込むことは考えにくいと言えます。大病院では少しつながっている部分があるので、遠くない将来に被害が出ることは十分に考えられます」

**尾尻**　「ランサムウェアでは、当事者同士で解決してしまうのですか」

**名和**　「そういうこともあります。アメリカの大学が攻撃され、数百万円で解決した例があります。マフィアが行うビジネスのモデルになっていて、金を取るのが目的なので、金さえ払ってくれれば解除するのです。ただ、そのような解決の仕方が勧められているわけではありません。インターポール（国際刑事警察機構）は攻撃者を見つけるのがミッションなので、見つかるまでは簡単に金を払わず、攻撃者側とのやり取りを続けてほしいと言っています」

**尾尻**　「名和先生はインターポールと協力して、サイバー攻撃の犯人を特定して逮捕につなげた経歴をお持ちですが、攻撃者の特定までにどのくらいの期間がかかるのですか」

**名和**　「短いものは2日、長いものは5年かかりました。2日で特定したのは、ベトナムの空港をハッキングした個人の攻撃者で中国人です。名前、身分証明書番号、携帯電話番号が分かったのはもちろん、スマートフォンに入っていた全ての写真も明らかになっています。そのくらいのことは簡単に出来てしまうので、皆さんもスマートフォンに入れる写真には注意してください。日本製のものに比べ、中国製のものはやりやすいそうです。こうした犯人とは違い、国家レベルのサイバー攻撃者は顔が見えません。大変苦戦しているのが現状です。

## 勉強会に引き続き、意見交換が続いた懇親会

※写真の氏名は敬称略とさせて頂きます。

懇親会で挨拶する山口和之・参議院議員（理学療法士）

乾杯の挨拶をする篠原裕希・篠原湘南クリニックグループ理事長

右から（以下同）堤治・山王病院院長、草野敏臣・ミッドタウンクリニック理事長

大津、堤、原田

名和、飯白敏晃・東京ミッドタウンクリニック統括事務長

瀬戸暁一・総合南東北病院BNCT研究センター長、冨岡、山口