核物質管理センター記者会見録

- 日時：平成28年５月18日（水）12：00～
- 場所：原子力規制委員会庁舎　記者会見室
- 対応：村上公益財団法人核物質管理センター理事長ほか

＜質疑応答＞

○司会　それでは、お伝えしているお時間が参りましたので、これより公益財団法人核物質管理センターにおける情報セキュリティ対応の不備に係る記者会見を行います。

まず、核管センターより一言冒頭にお願いします。

○村上公益財団法人核物質管理センター理事長　核物質管理センター理事長の村上でございます。

この度は、核物質管理センターの情報セキュリティ対応の重大な不備によって情報流出の可能性をもたらせ、指定機関としての信用を失墜させたことにつきまして、原子力規制庁、関係諸機関並びに皆様に多大なる御心配、御迷惑をおかけしたことについて、深くおわび申し上げます。

○司会　それでは、今日、委員会でも説明がございましたけれども、まずは調査報告の概要について、ポイントを絞って御説明をお願いします。

○村上公益財団法人核物質管理センター理事長　それでは、調査報告の概要について御説明いたします。

概要の目的ですけれども、２．にありますように、センター内において調査・検証の実施体制を設け、情報システム全体の包括調査と、関連するPC及びサーバ等の網羅的な調査・検証を行いました。特にセキュリティ専門会社による支援をもとに、ファイアウオール等のログの調査、ブラックリストの通信先の照合、フォレンジック調査等の技術的調査を実施いたしました。それとともに職員へのヒアリング等も行いました。

調査結果として主に以下の点が判明いたしました。

１、本年１月に報告しましたファイル共有ソフト「Xunlei」として探知された通信については、当該PC１台のソフトに製品として組み込まれたファイル共有ソフトが原因で通信が発生したと考えられます。この通信によりセンターが保有する情報の一部が流出した可能性がありますが、PCのクリーンインストールやProxyサーバ等が当時設置されていなかったということで、その内容を特定することはできませんでした。

なお、情報セキュリティ専門会社によりますと、当該通信のアップロード量から考えて、業務ファイルそのものが流出した可能性は低いという見解でございます。

（２）過去にセキュリティ監視機器（UTM）がファイル共有ソフトによるものとして検知した通信が複数のPCからございました。これらの通信にはファイル共有ソフト特有の通信が見られなかったこと等から、ウエブ閲覧をしたことの誤検知であるという可能性

が高いとセキュリティ専門会社からの報告でございます。

しかしながら、このファイル共有ソフト特有の通信以外で通信をした可能性ということも排除できないということで、情報の一部が流出した可能性は残るということでございます。

３点目として、情報セキュリティ会社が保有するブラックリスト、センターのProxyサーバ及びファイアウオールのログを照合した結果、マルウエア感染による通信は確認されませんでした。ウエブ閲覧の履歴又はPCの情報、メーカーの名前であるとか、シリアルナンバー等が流出した可能性はあるものの、先ほどと同様、業務データそのものの流出につながる痕跡は確認されませんでした。また、ほかのファイル共有ソフトがインストールされた形跡もございませんでした。

４番目として、情報セキュリティ会社によれば、ADサーバのフォレンジック調査の結果及び上記の痕跡がなかったという結果、更に常時監視の結果に基づくと、現時点でのセンターの情報システムは健全な状態にあるという報告でございました。

５番目としまして、そのほかの事象として、過去に検知された通信等について規制庁へ報告を怠っていた事象がございました。これらを含めて今回報告をいたしました。具体的には、UTMによる「eDonkey」等のファイル共有ソフトによる通信として検知された事象、もう一つ、昨年２月にDNSサーバがDDoS攻撃の踏み台となったという事象がございました。これらを含めて今回御報告いたしました。

次に、概要版３、概要版４に原因究明あるいは再発防止策等について結果報告をしております。

再発防止策については、特にセキュリティ体制の強化として、組織体制の整備と情報セキュリティマネジメントの導入を行うと。

２点目として、情報セキュリティシステムの強化として、ネットワークの分離と物理的な防護策の適用、システム運用体系の改善とIT製品のセキュリティチェック等を行う。

３点目として、情報セキュリティの意識改革と行動の徹底として、最新の情報収集と情報共有の実効性の向上、あるいは教育訓練の強化等を目指してまいります。

今後の対応としては、情報セキュリティ対策の専門家の知見を十分に活用して情報システムを構築していくとともに、外部有識者からなる第三者委員会を設置して、客観的・専門的見地から改善すべき問題点と再発防止策の実効性について評価をしていただく所存でございます。

本件につきましては､役職員一同責任の重大さについて深く反省をいたしております。理事長をはじめ役員及び関係職員の責任につきましては、役員の報酬の自主返上を含む役員と関係職員の厳重注意処分を行いました。本件を真摯に受けとめ、指定機関の使命と責任を再認識するとともに、指定機関としての責務の遂行と信頼回復に努めてまいりたいと考えております。

以上でございます。

○司会　それでは、皆様からの質問をお受けしたいと思います。所属とお名前をおっしゃってから、質問の方をよろしくお願いします。

それでは、質問のある方は手を挙げてください。

トミタさん。

○記者　朝日新聞のトミタと申します。

１点お伺いしたいのですけれども、３月31日に最初の報告書を報告された際なのですけれども、規制庁の方に報告されたときに、どのような報告をされて、どのような点が足りなかったかというのを具体的に教えていただければと思います。

○横田公益財団法人核物質管理センター理事　情報管理責任者の横田でございます。

１月の報告では調査・検証に２～３ヶ月かかるということを想定しておりますということを説明させていただいたところだったのですけれども、３月末に一部の調査について、特にファイアウオールのログとブラックリストとの照合の部分について、３月末までに終了しなかった。４月の頭になってしまいました。その部分が調査中ということで報告書には書かせていただきました。

それから、このファイアウオールログとブラックリストの調査の過程で、マルウエアの感染の疑い、それから、アドウエアの存在が確認されまして、それらの更なる調査、物によってはフォレンジック調査も行いまして、それが終了したということで、大変遅くなりましたけれども、今月12日に補正報告書ということで出させていただきました。

それから、報告書全般なのですけれども、これは３月末に出させていただいた報告書の内容が十分でない部分もありましたので、その部分を補足し、それから、正確にまた御理解いただけるように改めた部分、それから、誤記訂正、表現の適正化等を含めて補正報告書を出させていただきました。

○司会　ほかにございますでしょうか。

続けてトミタさん。

○記者　内容が不十分だったというのは、対策とかももちろんそのときに書かれたのかなと思うのですが、そういう点が足りなかった部分というのもあったのでしょうか。

○横田公益財団法人核物質管理センター理事　はい。対策の大きなところは大きく変えておりません。ただ、追加調査の中で出てきたものに対する原因、それから、それに対する対策ということで、そこは書き加えてございます。

○司会　ほかにございますでしょうか。

シゲタさん。

○記者　NHKのシゲタと申します。

何点かお伺いしたいのですけれども、特に一番危惧していたのが、重要な情報は漏れていないかどうかという点だったのですけれども、この点は漏れていないという理解でよろしいのでしょうか。

○横田公益財団法人核物質管理センター理事　センターが保有する管理すべき情報、いわゆる機微な情報については、情報そのものが漏れた可能性は低いということでございます。漏れていませんと言い切れないところは、これは過去の部分、古い２～３年前の情報というか、検出したということもございまして、フォレンジック等を行っても、その部分、そこにかかわるデータの部分が上書きされている可能性であったり、それから、ちょっと細かな話になるのですけれども、ファイル共有ソフトですね、これの存在というのは、１月にお話ししました「Xunlei」というP2Pがあるのですけれども、それについては、P2Pの通信、先ほど説明しました特有の通信、「ネーティブ通信」というのですけれども、特殊なポート番号を使った通信、これが「Xunlei」については検出されていましたので、それはP2Pによる通信と。

そのほかの通信と検知されたものにつきましては、調査等の結果、ウエブ閲覧の可能性が高いということでございました。ただ、P2P特有の通信というのは、ウエブにアドオンした場合にP2P特有の通信を使わないというケースがあるというふうな調べがありました。現在のところ、ウエブブラウザのアドオンについては、そのようなものが入っていないことは確認したのですが、検出された当時、その状況であったかどうか、過去にさかのぼってそこは調査できませんでしたので、そういう観点からあらゆるケースを考えると、完全に情報が漏れませんでしたとは言い切れませんでしたので、管理情報が流出した可能性は低いというふうに報告させていただきました。

○記者　済みません、今の点なのですけれども、いつまでをさかのぼることができて、いつより前がさかのぼることができなかったのかということと、先ほど冒頭に機微な情報とおっしゃったのですけれども、その中にそれこそプルトニウムにかかわるような情報とかというのは含まれていないと考えていい理由は何なのですか。

○横田公益財団法人核物質管理センター理事　ファイアウオールのログからいきますと、平成25年４月19日までさかのぼっております。機微な情報を我々は「管理情報等」と呼んでいますけれども、その中には、保障措置検査の関係で事業者から報告していただいたプルトニウム量、それから、検査した際のプルトニウム量等については、それは管理情報等として管理しております。今回の情報の流出の可能性といったところでは、そのような情報が流出した可能性は低いというふうに考えております。

○記者　今のところをもう一度確認したいのですけれども、機微な情報が流出した可能性は低いけれども、否定できないという話だったと思うのですけれども、機微な情報だけではなくて、プルトニウムの量とか、検査でプルトニウム量を量ったりすると思うのですけれども、そういった情報も流出した可能性は否定できないということですか。重要な情報も流出した可能性は否定できないということですか。

○横田公益財団法人核物質管理センター理事　否定できない。

○記者　可能性があると言ってもいいのですけれども。

○横田公益財団法人核物質管理センター理事　低いといえども100％言い切れないところ

でございますので、可能性は残ります。流出した可能性は残る。いろいろなケースを考えると、そういうことでございます。

○記者　分かりました。

最後に、これは規制庁側になるのですけれども、最後、委員会の中で田中委員長が、規制庁も含めて、今回のことを糧にして今後対策を考えてもらいたいというふうに言っていたのですけれども、これは一つの指示というふうにも受けとめられるのですけれども、どういうふうに受けとめられていらっしゃいますか。

○粂川長官官房放射線防護グループ放射線対策・保障措置課保障措置室長　今回の事案を受けまして、核物質管理センターにおける情報セキュリティの状況というのを、我々、十分知っていなかったということは反省点だと思っています。これから、今回の調査では原因究明と再発防止対策というものを策定されていますので、それをきちんと実施していくか、その部分を我々としても見ていく必要があるということで委員会には御報告して、それをきちんとやっていくようにというのが委員長からの御指示だったと理解しております。

○記者　今の確認なのですけれども、僕の受けとめとしては、核管センターに対してだけではなくて、もっと広く全般的に核セキュリティ、情報セキュリティをしっかりしていけというふうに受けとめたのですけれども、そういう意味ではないということでしょうか。

○粂川長官官房放射線防護グループ放射線対策・保障措置課保障措置室長　広くとおっしゃるのは、どういう意味での広くでしょうか。

○記者　核物質を扱っているのは核管センターだけではなくて、いろいろな様々な施設とか機関があると思うのですけれども、それも含めて全般的にサイバーセキュリティをめぐる対策をしっかり講じて考えていけという指示ではないということですか。今回の件のみに関する指示だということですか。

○粂川長官官房放射線防護グループ放射線対策・保障措置課保障措置室長　原子力施設等におけるいわゆるサイバーセキュリティとか、そういった部分というのは別の部署で担当しております。我々は保障措置を担当しておりますけれども、保障措置においては、様々な保障措置に関する情報を事業者から提供を受けまして、核物質管理センターに指定情報処理機関として情報の処理を委託しております。また、保障措置の実施に当たっては様々な情報を扱います。そういったものを核物質管理センターできちんと指定機関にふさわしい形で厳密に管理していただくというのが我々の問題認識でございまして、基本的にはその部分できちんと対応していくようにということを委員長の方から御指示があったものと私の方では理解しておりますが。

○司会　ほかにございますでしょうか。

カンダさん。

○記者　時事通信のカンダです。

２月の踏み台の方なのですけれども、これはDNSを使ったリフレクター攻撃とか、そういうものに使われたのではないかということだと思うのですが、結局、これに関しても、その前のファイル共有ソフトのときと同じように、最終的には横田さんのところに報告が行って、横田さんのところでとまっていたという理解でいいのですか。

○横田公益財団法人核物質管理センター理事　はい。そのとおりでございます。

○記者　それで、この際も、前回１月のときも、重要な情報が出ていないと見られるということから報告をなされなかったと思うのですけれども、このときも同様の判断をされたということですか。なぜそこでとめてしまったのか。要するに規程があって、不正アクセスがあった場合は報告しなければいけないということにはなっていたわけですよね。それに明確に該当すると思うのですけれども、これがまた横田さんのところでとまってしまったというのは、これはどういう理由なのですか。別の理由があるのですか。

○横田公益財団法人核物質管理センター理事　別の理由はございません。責任者である私が情報管理の重要性に係る認識、これが全く不十分、それから、情報セキュリティに対する意識、これが低かった。それよりも欠如していたということが根本にあります。もしそこで国に報告しなければという、頭にそういう意識があれば、そのようにしたと思います。大変私の不徳のいたすところでございますけれども、そういう意識にも至らなかった。つまり意識が全く欠如していたということが理由でございます。

○記者　今後、再発防止策の中で役員によるリーダーシップの発揮とコミットとか、いろいろ書いてあるのですけれども、引き続き横田さんが情報管理に関しては責任者を務められるということでいいのですか。

○横田公益財団法人核物質管理センター理事　それについては、まだもちろん今の時点で決まっておりません。私の処分ももちろんありますし、私がこのままCIOを続けるかどうか、これも決まっておりません。私としては、私よりも適切な人がいれば、きちんとその方に引き継げればというふうには思っておりますけれども、私も、一方で今、責任を逃れるというか、責任逃れするつもりはございません。きちんと私がそれを、もしそういう適任者がいなければ、私がそれを果たさなければいけないという使命も今の私には負っているかと思います。これは今後、組織、それから規制庁さんを含めて最終的には決定されることだと私は思っています。

○記者　横田さん個人の問題というよりは、かわりの方が仮に例えば同じ立場に立ったとして、また同じ間違いを犯す可能性というのもないわけではないと思うのですね。そこは、だから、御本人の、経営層の意識を高めるというのが一つの対策だと思うのですけれども、それ以外に、例えば責任者の方が１人で判断しないような仕組みというのはちゃんと構築できて、どういうふうに人的な仕組みとしてはこれを防ぐことができるようになっているのかというのを具体的に説明していただきたいのですけれども。

○村上公益財団法人核物質管理センター理事長　お答えします。

今回の事象は、個人の責任というよりも核管センター全体の組織としての認識が足りなかったと、あるいは危機に対する意識が低かったということだと思います。今後の対策としては、まず職員の意識の改革をするということ、それと、組織体制として以前は情報セキュリティに対しての臨時的な組織しかなかったものを、専門の専従の情報セキュリティ室を作る。あるいは内部規程も規程上は存在していましたけれども、その下の手続上、更にもっとしっかりとしたものを作っていく必要がある。あるいは先ほどから言っている組織の認識あるいは問題点の根本には、PDCAの特にチェック機能と改良の部分がしっかりと実施されなかったというふうに組織として考えていくということを含めて、再発防止策を検討いたしました。

それともう一つ、もちろん非常事態というか、今回のようなときにどう対応するかということも不足であったと考えておりますので、その点も含めて再発防止策を作成いたしました。

○記者　それから､最後に１つだけ｡先ほどちょっと処分という話が出たのですけれども、結局、本件については、今の時点でまだ最終的な処分とか、そういったものというのはまだなされていないのでしたか。

○村上公益財団法人核物質管理センター理事長　いや、処分はいたしました。役員の報酬の返上と、あと、役職員の厳重注意を含めて文書で処分をいたしました。

○記者　今後、今日、報告書が提出されて、一応、内容は規制委員会の方から了承を得たということで、最終的な処分というか、更に何かされるということはお考えなのでしょうか。

○村上公益財団法人核物質管理センター理事長　今回の処分が報告書を提出してから処分をしたということで､今回に含まれていることを一応鑑みて処分をいたしました｡ただ、もう一つ、本件に関連してということもあるのですけれども、役員３人の任期満了ということもあり、一応、役員の公募を今しております。特に今回のことがということではなく、公益法人として役員は独立法人、独法と同様に再任の場合には公募をするということに基づいてやっております。

○司会　ほかにございますか。

タケオカさん。

○記者　共同通信のタケオカと申します。

これまでの質問とちょっと関連するかもしれないのですが、PCはクリーンインストールしたので、情報の内容を特定することができなかったとあるのですけれども、その前段のところで情報の一部が流出した可能性というのが付いているのですが、ここはあくまで可能性がつくのか詳しく教えていただきたいのですけれども、データが流出したのは事実だけれども、そこに有意な情報が入っているかどうか分からないということなのか。

○水原公益財団法人核物質管理センター総務部長　総務部長の水原でございます。

今の御質問なのですけれども、確かにファイル共有ソフトによって通信が行われたのは事実でございます。その中身は、ファイアウオールのログで確認をするしか、当時、ありませんでした。ファイアウオールのログでは、その通信の中身、細かいところまで分からないということで、どういったものが通信によってアップロードされたのかというのが分かりませんでした。ということですので、可能性はあるということなのですけれども、アップロードの量から、ファイルが流出したような量ではないということを情報セキュリティの専門会社にお願いをして分析していただいております。その結果から、業務上のデータについては出ていないのではないかという見解を頂いておるといったことでございます。

○記者　あともう一点、処分なのですけれども、理事長は例えばどのような処分内容なのでしょうか。

○村上公益財団法人核物質管理センター理事長　具体的には３人の理事、理事長も含めて報酬の返上ということで、私が20％返上、理事が10％返上ということでございます。

○記者　先ほど任期満了という話がありましたけれども、現時点ではこの処分、報酬を返上された方は理事の職にはないということなのですか。

○村上公益財団法人核物質管理センター理事長　私を含めて３人理事がいる。その３人全員が報酬の返上をいたしました。

○記者　任期満了で公募という話がありましたけれども、これは任期満了はこれから迎えるということなのですか。

○村上公益財団法人核物質管理センター理事長　この６月の終わりで任期満了になりますので、先ほど申し上げたように、この事象が原因ということではなく、それも含めて、一応、独立法人、独法に従って、任期満了の場合には公募をするということがありますので、今回は理事３人の公募を今しているところでございます。

○記者　20％、10％は何ヶ月分とか、月額分とか。

○村上公益財団法人核物質管理センター理事長　月額です。

○記者　１ヶ月に対して20％と10％をそれぞれ減額ということですか。

○村上公益財団法人核物質管理センター理事長　そういうことです。

○記者　分かりました。

○司会　ほかにございますか。

オオヤマさん。

○記者　読売新聞のオオヤマと申します。

新たに分かっていて報告していなかった事象というのは、２ページの（５）と（６）の分ということでよろしいですか。

○横田公益財団法人核物質管理センター理事　（５）につきましては、UTMという監視装置

があるのですけれども、その監視装置の結果としてファイル共有ソフト「eDonkey」、済みません、「等」というのが抜けていますけれども、「eDonkey」その他ファイル共有ソフトと思われる検知された通信、これについては国に１月にも報告しておりませんでした。

それから、（６）について、これにつきましても１月には報告しておりませんでした。DDoS攻撃の踏み台についても。

以上でございます。

○記者　これを把握されたのはいつなのですか。それと、１月の時点で把握していたのでしょうか。把握していたとしたら。

○横田公益財団法人核物質管理センター理事　いや、把握しておりました。

○記者　把握していたのにもかかわらず、報告しなかったのはなぜですか。

○横田公益財団法人核物質管理センター理事　それは先ほどと同様でございますけれども、国に報告しなければならないと、そういった意識に欠けていた。つまり重要性に関する認識とか意識が欠如していたということに尽きます。

○記者　そういうのもあって、でも、問題だと思ったから１月に公表されたのですよね、最初の「Xunlei」の件は。何で「Xunlei」のことは発表したのに「eDonkey」に関することは発表されていなかったのですか。

○横田公益財団法人核物質管理センター理事　済みません、これにつきましては、そのときに過去の部分について頭に浮かびませんでした。これは本当にそのときに報告しておけばというふうに猛省しております。

○記者　頭に浮かばなかったということなのですけれども、把握していたけれども頭に浮かばないというのは理解できないのですけれども。

○横田公益財団法人核物質管理センター理事　その時点では報告しなければという方向に頭が行かなかったということでございます。

○記者　ちなみに、この「eDonkey」による通信というのも情報流出はないというふうに見ていらっしゃるのですか。

○横田公益財団法人核物質管理センター理事　可能性が低いということです。

○記者　それも「Xunlei」と同じ理由でということですか。ファイル量が少ない、小さいということからですか。

○横田公益財団法人核物質管理センター理事　これは概要版の１ページの（２）の部分でございます。これについては、ファイル共有ソフトP2Pによるものとして検知された通信なのですけれども、特有のネーティブ通信、これは通常の80番ポートではなくて、それぞれのP2P固有のネーティブ通信を普通行います。それが見られなかったこと、それから、ウエブブラウザにファイル共有ソフトがアドオンされていなかったこと等ありまして、ウエブ閲覧を誤検知した可能性が高いということで、センターが保有する情報そのものが流出した可能性は少ないだろうと、低いだろうということでございます。

○記者　あと、済みません、この「eDonkey」というファイル共有ソフトがインストールされていたパソコンと「Xunlei」とは別ですか、それとも一緒ですか。
○横田公益財団法人核物質管理センター理事　別です。
○記者　別で、どういった経緯でこの「eDonkey」がインストールされていたのですか。
○横田公益財団法人核物質管理センター理事　「eDonkey」そのものはインストールされた形跡はありません。P2PとしてPCにインストールされたというのは、（１）の１台のPC、「Xunlei」として検知された通信、これを発生させた１台だけでございます。
○記者　ということは「eDonkey」はどこか別の場所にというか、別のサーバなりなんなりにあって、パソコンそのものにはないけれども、「eDonkey」の作用によって情報というか、いろいろとデータのやり取りがあって、それが誤検知されたという、そういうことですか。
○横田公益財団法人核物質管理センター理事　我々の調査､専門会社の報告等からすれば、これは「eDonkey」そのものの通信ではなくて、UTMという総合脅威管理機器というのがあるのですけれども、それのシグナチャー（signature）からその通信を「eDonkey」として誤検知したということでございます。
○記者　あと（６）の件なのですけれども、指摘してきた外部機関というのはどこで、あと、実際に踏み台としてどこか別の機関に被害を与えた可能性があると思うのですけれども、実際に被害があったのか、ないのか。攻撃先の機関というのはどちらなのでしょうか。
○横田公益財団法人核物質管理センター理事　通報があった外部機関というのはJPCERTコーディネーションセンターというところでございます。これはインターネット上におけるコンピューターセキュリティインシデントについて、国内の組織及びユーザーに関する技術的な支援を行うことを目的とした一般社団法人でございます。
　それから、その攻撃を向けてしまった、つまり相手ですね。相手については、ここはJPCERTからはお聞きしましたけれども、そこについては教えていただけませんでした。
○記者　あと、委員会でも質問されていたと思うのですけれども、大抵こういうものというのは、パソコンにマルウエアなりなんなりが仕込まれていて、それで遠隔操作されるというケースが多いと思うのですけれども、そういうことはなかったのですか。
○横田公益財団法人核物質管理センター理事　これにつきましては、JPCERTに確認してもらいまして、我々核管センターのDNSサーバの脆弱性、これは外からの問合せに対して再帰的な回答を続けるという設定があるのですけれども、そこが我々に脆弱性があってそのまま再帰的な回答を続けるような設定になっておりました。このミラーという､「リフレクター」というふうに呼ばれている部分なのですけれども、ここについては指摘を受けて､専門会社に設定の変更等を聞きまして､それで設定の変更をしました。それで、JPCERTからそこを確認していただいたということでございます。
○記者　分かりました。ありがとうございます。

○司会　ほかにございますでしょうか。
　シュゾウさん。
○記者　毎日のシュゾウです。
　２番の（２）の「ファイル共有ソフトによるものとして検知した通信が複数のPCから多数」というのは、これは正確な数字を教えてもらえますか。
○水原公益財団法人核物質管理センター総務部長　IPアドレスからいくと17IPアドレスなのですけれども、その中には、NAT変換をするということで代表するIPアドレスで複数台のPCを１個のIPアドレスで共有しているものもありますので、それを含めると約40台になります。
○記者　多数というのは何回ですか。
○水原公益財団法人核物質管理センター総務部長　約8,000回でございます。
○記者　（５）との関係ですけれども、「eDonkey」を検知したというのもこの１つということですか。要はファイル共有ソフトは実際には入っていなかったのに、UTMがファイル共有ソフトですと通知してきたというのがこの結果なのですよね。（５）の「eDonkey」も、結局、この一種だったという、そういうことですか。
○水原公益財団法人核物質管理センター総務部長　はい、そうです。
○記者　（５）の結果だけ、たしかセンター内に通知を出していますよね。これは何でなのですか。8,000回もあったのに、なぜこの１回だけ通知が出たのか、そこをちょっと事実関係を教えてもらえますか。
○横田公益財団法人核物質管理センター理事　当時、このUTMの報告がありまして、それに基づいて当方の業務連絡帳等でこのファイル共有ソフト「eDonkey」等の使用を禁止、それは元々禁止しているのですけれども、それとアンインストール等を周知させました。当時のファイアウオールのログというのを核管センターの中で通信元、通信先というのは分析することができておりませんでした。そういうことで通信先を特定できないものですから、センターの中全体にそういった周知文書を出したということでございます。
○記者　いや、お聞きしているのは、残りの8,000回のやつはUTMから検出されましたよという話が来ていたのに、要は、逆に言うと、何も対応をとらなかったということなのでしょうか。要は、なぜ40台の8,000回のパソコンがファイル共有ソフトを検知しているという事実があったのに、「eDonkey」を誤検知したという１回だけ対策をとったということなのか、そこをちょっと教えてほしいのですけれども。要は残りの8,000回は放置していたということなのですかね。
○横田公益財団法人核物質管理センター理事　それにつきましては、素直に言えば、我々の認識、意識が低くて、そこをきちんと対応していなかったということでございます。
○記者　だから、この１回だけ逆に指示を出したというのは、というか、通知を出したというのは、何かこの１回が特別なものだったということなのでしょうか。それとも通知

を出したのはほかにもあるのですかね。

○横田公益財団法人核物質管理センター理事　このUTMが検出したP2P関係につきましては、２回ぐらい出しているかと思います、通知を。

○記者　それは何月と何月でどんな通知ですか。

○横田公益財団法人核物質管理センター理事　27年１月30日と27年９月15日に出しております。

○記者　９月の件は今回の「Xunlei」の件ですか。

○水原公益財団法人核物質管理センター総務部長　９月の件は「Xunlei」をきっかけに通知を出させていただきました。

○記者　１月の件はこの「eDonkey」の件ですか。

○水原公益財団法人核物質管理センター総務部長　はい、そうです。

○記者　そうすると、質問の意味がまたあれなのですけれども、要は、そのほかの件については放っておいていたという認識なのですか。要は8,000回検出しているのですよね。だけれども、センター内にこのファイル共有ソフトの感染に気をつけましょうとか、削除してくださいとか、検出されていますよという通知は「Xunlei」と「eDonkey」の２回だけだったということは、ほかは放っておいていたということなのですかね。なぜこの「eDonkey」の件だけ通知が出たのかというのがよく分からないのですよ。

○村上公益財団法人核物質管理センター理事長　今、実際に通知簿を見ているのですけれども、その段階では「eDonkey」だけということではなく、「eDonkey」ほかも含めて一般的なP2Pへの注意ということであったと記憶しております。

それともう一つ、8,000回というのは、今回の調査によって出てきた。その段階では、それだけのナンバーが出ているということは承知しておりませんでした。先ほど申したように、去年の８月から常時監視が始まって、あるいは今回の調査で初めて出てきたということでございます。

○記者　では、済みません、８月以前はこのUTMというやつがファイル共有ソフトの検知をしていましたということ自体、全然知らなかったということなのですかね。それともそれは知っていたけれども、特に対策をとらなかったということなのですかね。それはどっちなのですか。

○横田公益財団法人核物質管理センター理事　UTMで報告を受けておりまして、承知しておりました。対策をきちんと講じておりませんでした。

○記者　分かりました。

もう一個いいですか。このDDoS攻撃の踏み台とあるのですけれども、踏み台というのは何ですか。もうちょっと分かりやすく説明してもらえますか。何か使われたのですかね、ここから大量のアクセスを出す何かに。

○横田公益財団法人核物質管理センター理事　私どものDNSサーバを経由して、ある企業さんだか、組織だか、ちょっとそこは知らされていないのですけれども、あるところの情

報システムに攻撃をかけて、攻撃というか、相手に問合せを出し続けて、そこで相手の機能を失わさせる。つまり正規の機能を果たせないように邪魔をする。そういったことだと思います。

○記者　済みません、サーバを経由してというのがよく分からないのですけれども、このサーバ自身が攻撃を仕掛けていたということなのですか。それとも攻撃を仕掛けていた人がどこかにいて、その攻撃の内容がこのセンターのサーバを通過していたという、そういうことなのですか。それともこのサーバ自身が、要は大量攻撃を送りつけている発信元になっていたということもあり得るのですかね。

○横田公益財団法人核物質管理センター理事　これはうちのDNSサーバに対して､外からの攻撃者が悪意を持ってうちの脆弱性を突いて、うちのサーバが相手、相手というのは被害に遭われた相手の情報システムに通信を送り続けたということでございます。

○記者　では、その通信の出元はセンターのサーバなのですね。

○横田公益財団法人核物質管理センター理事　そのとおりでございます。

○記者　それはやはり何か操られていたというか、さっき御質問がありましたけれども、マルウエアみたいなものという可能性もあるのですけれども、それは全然なかったというのはどういう仕組みなのでしょうかね。

○横田公益財団法人核物質管理センター理事　これにつきましては、先ほどのJPCERTからお聞きしましたところ、我々のDNSサーバの脆弱性、再帰的な回答をしてしまうといったところを突かれ、その脆弱性を突かれて攻撃したものですというところはJPCERTの方で確認して、説明を受けました。我々のところに特にマルウエアが入って、我々のDNSサーバ自体がそういった活動をしたのではなくて、外からの脆弱性によって我々がリフレクターになってしまったということなので、我々、これまでの経験から、こういった状況において情報流出、そのリフレクターになった部分、DNSサーバ、そのシステムにおいては情報流出につながることは今までありませんというふうにお聞きしています。

○記者　いや、今までは多分被害者だったのですけれども、この件は加害者になっているのですよね。そういうことですよね。その際、要は別に被害者がいるわけで、相手が誰だか分かりませんからといって放っておいていいのですか。

○村上公益財団法人核物質管理センター理事長　２点ほどあると思います。

１つは、加害者になったというか、利用されてもとの加害者の踏み台になったということで、それはコンサルタントのその後の処置によると、どうもDNSサーバの設定が外からのアタックというか、利用することを防ぎ切れなかったということで、設定を変更してその後は異常がないと。かつ、また情報の流出がないと。

その相手方に対しては大変申し訳ないのですけれども、先ほど言ったように、そこがどこであるかということを当センターとしては知らないというか、教えていただけなかったということで、これ以上のことができなかった。

この件の一番の問題は、これほど重要なことを報告しなかったということだと思うの

です。ですから、その点は、先ほども言いましたように、組織全体としてのこういうセキュリティ、あるいはこういう機関に対しての認識が非常に甘かったというふうに反省しております。その意味でここに列記したというか、明記をさせていただきました。

○司会　ほかにございますでしょうか。ほかはございませんか。よろしいですか。

それでは、本日の会見はこれで終わりにしたいと思います。お疲れさまでした。

－了－