

防衛関連団体も標的

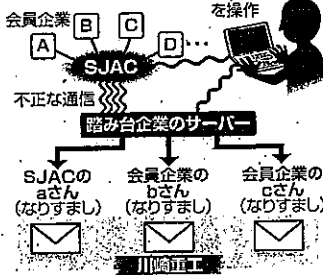
情報集め 加盟社にウイルス

サイバー攻撃

防衛産業大手「三菱重工」(東京都)へのサイバー攻撃発覚に続き、防衛装備品メーカーのトップらが役員を務める「日本航空宇宙工業会」(同・SJAC)のコンピュータも、情報を抜き取るタイプのウイルスに感染していたことが14日、わかった。同会から窃取されたメールにウイルスが仕込まれ、会員企業の川崎重工(神奈川県)に対する標的型メール攻撃に転用されていたことも判明。警視庁などは、攻撃者がSJACを起点として防衛産業に感染を浸透させ、幅広い情報を抜き取ろうとしたとみて調べている。

▲業界団体の甘さ突く攻撃39面

▲SJACを介して行われたとみられる標的型攻撃の一例



関係者によると、川崎重工で、「一括調達に係るコメント」などの題されたファイルも添付。本文は幹部が先となっていたSJACの同僚のパソコンがウイルスに感染しており、メール内容などの情報が外部から抜き取られていたという。川崎重工は今年6～7月にも少なくとも2度にわたる標的型メールを受け、SJACの会員企業で、航空機

部品加工などを手がける神奈川県内のメーカーの担当者を送信者として偽装していたという。

メールは、東京都中央区にある国際電話サービス会社から送信されていた。警察当局が同社のコンピュータを調べたところ、ウイルスに感染し、攻撃者が身元を隠すための「踏み台」として使われていたことが発覚。知らない間にSJACとの間で不正な通信が行われていたことも分かった。

SJACによると、同会には三菱重工や川崎重工、IHIなどの大手防衛装備品メーカーや航空・宇宙関連産業の9社が「正会員」に、海外から防衛装備品な

どを輸入している商社などを登録している。警察当局で現在、通信記録などを調べているが、SJACのコンピュータは感染してかなりの期間が経過しており、長期にわたって会員企業とのメール内容

などを盗み見られていたとみている。警察当局幹部は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

警察当局は「攻撃者がセキュリティの甘い業界団体を狙い、ここを突破口に防衛業界全体にウイルス感染を広げようとしたのではないか」としている。

業界団体の甘さ突く

防衛関連産業 サイバー攻撃 会員企業の社員かたる

日本の防衛秘密を狙う攻撃者は、セキュリティの甘い業界団体に狙いを定めた。防衛産業大手「三菱重工」で発覚した攻撃と同様のサイバー攻撃は、社団法人「日本航空宇宙工業会」(東京都・SJAC)

を起原に業界全体に広がりつつあった。名前をかたられた会員企業の社員らは「知らないうちに名前が使われた」と一様に驚きの表情を浮かべた。

「まさかこんな問題が」(本文記事一面) 担当者とすると、同会ではパソコンなどにウイルス対策ソフトを入れているものの、それ以上の対策は講

じておらず、ネットワークに不正侵入があっても、記録が残る仕組みにはなっていない。当会で扱った情報は基本的に公表されるものが多く、強固なセキュリティは不要だと思っていたと釈明する。

だが、関係者は「攻撃者が狙ったのは、同会の人的ネットワークだったので、標的型メールに名前を使

助会員も含めると約140社のほり、各社からの出向者で構成される職員は日常的に、計数百人とメールのやり取りをしているとい

こうした情報を盗み取れば、防衛産業にかかわりの深い人物のメール情報を自在に抜き取ることが可能で、それらの人物になりすまして、標的型メールに利用するとも容易

われていた人物は、外部から指摘を受けるまで全く気づかないケースが多い。神奈川県内の航空部品加工会社のOB(63)もその一人だ。

社内の技術担当者から「川崎重工に送りつけられたウイルス付きメールに名前が使われている」と連絡があったのは今年7月頃。知人から定期的にメールで受け取り、仲間に転送している業界情報が、知らないうちにウイルスを仕込まれ、川崎重工社員あてに送信されていたというのだ。しかし、自分のメールの通信履歴には送信の記録はなく、「全く心当たりがない」と首をひねる。

この部品加工会社では、3月の東日本大震災後、会社の部署アドレスから知らない間に外部に約120通のメールが送信されるなど

トラブルが続いた。社員らに聞き取りを行ったが「結局、何が起きているのかわからなかった」という。今回の件を受け、SJACは不正な通信を監視する新システムを導入するとい

う。警察当局の幹部は「社だけセキュリティ強化に努めても、関係先の対策が甘ければ感染を広げてしまう。社会全体で危機意識をもたなくては」と話す。

防衛関連団体も感染

サイバー攻撃 会員企業の情報盗む？

三菱重工工業のサービーカーなどの業界団体 を盗み取るタイプのウィルスに感染していたことが同会のコンピューターがサイバー攻撃を受け、「日本航空宇宙工業会」が15日、捜査関係者への取材で分かった。

警視庁などは、攻撃者が同会のコンピューターから盗み出した情報を基に、複数の会員企業にサイバー攻撃をくり返していた疑いがあるとして調べている。

SJACCのホームページによると、同会は航空

・宇宙機器関連メーカーなど140社で構成。三菱重工や川崎重工工業などの防衛装備品メーカーや航空・宇宙関連企業など91社が正会員、大手商社など49社が賛助会員として登録している。

警察当局が通信記録を解析したところ、同会のコンピューターは感染からかなりの期間が経過しており、長期にわたり会員企業とのメール内容などの情報が盗み取られていた可能性がある。

サイバー攻撃を受けた川崎重工にも8月26日、同会幹部名で標的型メールが送信された。資料「事前送付」とのタイトルで「一括調達に係るコメント」と題されたファイルが添付され、約10時間前に同会幹部が関係者に送信した文面がほぼそのまま引用されていた。捜査関係者によると、同会幹部が同報通信先と関係メールを送った同会職員のパソコンがウィルス感染しており、メール内容が外部に抜き取られたものとみられる。川崎重工には今年6～8月に禁

三菱・川崎重攻撃同一犯か

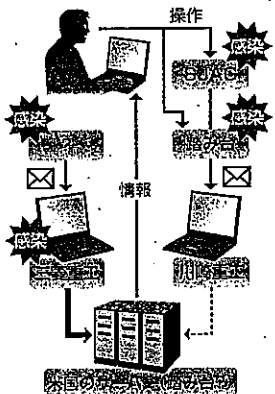
米サイトに強制通信

社団法人日本航空宇宙工業会(JAICA)を通じて川崎重工に標的型メールが送られていた問題で見つかったウイルスには、感染したコンピューターに米国内のウェブサイトを強制的に通信させる機能が埋め込まれていたことが15日、関係者の証言で分かった。このサイトは「三菱重工」で感染した端末の通信先と同一であることも判明。攻撃者が外部から端末を操作するための踏み台として利用していたとみられ、日本を代表する防衛大手2社が、同じ攻撃者に狙われていた可能性が浮上した。

警察当局は米國に協力を促し、二つの攻撃の関係を捜索する方針。情報源が「このサイトの通」

工には6〜8月、少なくとも3回にわたって、SJA職員や会員企業社員を偽装した標的型メールが送り

三菱重工と川崎重工への標的型攻撃のイメージ



「踏み台」調査必要
ウイルス対策会社「カスベルスキー」の前田典彦研究員の話「過去に別々の犯罪集団が偶然に同じサーバーを踏み台として使っていたケースもあったが、通常は攻撃ごとに踏み台を作る

ため、同じサーバーを異なる犯罪集団が共有することは少ない。同一犯の可能性が高まったことで、攻撃者が日本の防衛秘密を狙っていたとの意図はより明確になった。踏み台サーバーなどの通信履歴の早急な調査が必要だ」

報をやりとりするようプロプログラミングされたことが判明。指定された通信先を調べるべく、IPアドレスを調べるべく、インターネット上の住所が米国カリフォルニア州に

登録されたサイトだった。一方、三菱重工のコンピュータで感染が確認されたウイルスも、同種の機能をもち、中国やインドなどが

踏み台「サイバー攻撃の際、攻撃者が発信元を突き止めるには、攻撃の継続として利用するパソコンやサーバー、セキュリティ対策の甘いパソコンなどがウイルスに感染させられ、利用者が気づかないうちに遠隔操作される。今年3月、韓国の政府機関などの約40サイトがサイバー攻撃を受けた際、日本のパソコンなども踏み台として攻撃に参加させられたように、国境を越えて悪用されるケースも多い。

通信していたが、そのうちの一つが、このサイトだった。

このサイトも、何者かにウイルス感染させられ、外部から操られていた可能性が高いという。三菱重工へのサイバー攻撃が発覚した9月中旬以降に閉鎖された

「セキュリティ対策の甘いサイトをウイルス感染させ、踏み台として利用するが、目的を達したり、攻撃が発覚したりすると「使い捨て」にする。これも多いという。警察当局では、攻撃者が三菱重工や川崎重工から情報を抜き取るため、このサイトで情報のやりとりをした上で別のサイトに送っていたとみて、捜査を進めている。