

防衛産業へのサイバー攻撃について

1 三菱重工業の事案の概要（三菱重工業の説明による）

8月中旬 三菱重工業において、複数のコンピュータがウイルスに感染している可能性が判明、調査とウイルス駆除を実施。

8月下旬 感染の状況等について専門業者による調査を開始、爾後、警察当局に状況を報告。

9月19日 新聞報道（読売朝刊）、防衛省に状況を報告。

○ 複数の事業所のコンピュータ83台においてウイルス感染が判明。

○ 専門業者に調査を依頼したところ、

① 企業の情報を盗み出すことを狙ったウイルスである可能性が高いこと

② 一部のコンピュータのシステム情報が流出した可能性があること

③ 一部のコンピュータに外部から侵入された痕跡があること

等
が分かったため、警察当局に状況を報告。

○ 事実関係の調査が進められており、この結果についてはほぼ毎日報告を受けているが、現在のところ、製品や技術に関する情報のデータ流出は確認されていない。

2 他の防衛関係企業へのサイバー攻撃について

○ 報道にあったIHI、川崎重工業、三菱電機については、保護を要する情報の流出は確認されていない。

参考1：防衛省の調達における秘密等の保全及び情報セキュリティの確保について

参考2：三菱重工業発表資料

防衛省の調達における秘密等の保全及び情報セキュリティの確保について

1 省秘、防衛秘密及び特別防衛秘密

省秘、防衛秘密及び特別防衛秘密を扱う情報システムについては、秘密保全対策ガイドラインにおいて、秘密保全施設外への接続は、いかなる場合も禁止しているため情報の流出の可能性はない。

2 保護すべき情報（注意レベル）

保護すべき情報を扱う情報システムについては、情報セキュリティの確保に関する特約条項において、次の事項に関する手順や要領などを定め、情報セキュリティ対策を求めている。

○情報セキュリティ基本方針等の確認

○保護すべき情報の取扱い

（ウィルス対策ソフトウェア等により悪意のあるソフトウェアなどから保護）

○保護すべき情報の漏洩に関する契約企業の責任

○下請負者を使用する場合の確認及び届出

○監査

○事故発生時の措置

（適切な事故対処、速やかな報告、基本方針等の見直しに反映）

○契約企業の情報漏洩等における契約の解除

○契約履行後における契約企業の義務

参考：経緯

○平成16年4月 情報システム関連の調達に適用

○平成18年4月 航空機、航空機用エンジンに適用

○平成19年1月 誘導弾、誘導武器システムに適用

○平成19年4月 全ての装備品等の調達に適用

○平成23年4月 下請負者へも適用

3 今後の対応

事実関係の調査結果を踏まえ、再発防止の観点から、情報セキュリティの確保について必要な対策を講じる。

三菱重工発表資料

2011年9月19日

三菱重工業株式会社

本日の一部報道について

本日、当社のコンピューターがウイルスに感染しているとの一部報道がありました。

8月中旬にウイルス感染の可能性が判明し、その後ウイルスの特性により情報漏えいの危険性も判明したことを受け、その旨を警察当局に報告、相談するとともに、以後、外部の専門家と共同で調査、対応を進めております。

現時点ではウイルス感染による被害拡大は止まったものと考えております。

また過去に社内一部のコンピューターのシステム情報(ネットワークアドレス等)が流出した可能性があることは判明しているものの、当社の製品や技術に関する情報の社外へのデータ流出は現在確認されておりません。

これまでウイルス駆除などの被害拡大防止策を講じておりますが、今後とも引き続き調査を進め、対策強化をはかってまいります。

以上

平成23年9月30日

三菱重工業株式会社

コンピューターウイルス感染に関する調査状況について

8月中旬にウイルス感染の可能性が判明したことを受け、ただちにウイルス駆除などの被害拡大防止と監視・防御体制の強化の両面で対策を講じるとともに、外部の専門家と共同で詳細な調査及び必要な対応を進めております。現時点までの調査では当社の製品や技術に関する情報の社外へのデータ流出は確認されておりませんが、今回のサイバー攻撃の規模・悪質性に鑑み、当社は本事案について、本日警視庁に被害届を提出しました。

今後とも引き続き調査を進め、警察の捜査に全面的に協力してまいります。

また、当社は従来から自社の製品及び技術の重要性を認識し、高レベルの情報セキュリティを維持すべく取り組んでまいりましたが、このたびの事案を重く受け止め、さらなるセキュリティ強化に取り組んでまいります。

以上

2011年10月24日

三菱重工業株式会社

コンピューターウイルス感染に関する調査状況について(その2)

当社は8月中旬に、一部パソコン及びサーバーのウイルス感染が判明したことを受け、以降、外部の専門家と共同で詳細な調査を進めて参りました。これまで製品や技術に関する情報の社外へのデータ流出は確認されておりませんが、今般、製品や技術に関するデータの一部が社内のサーバー間で当社の意図しない形で移動していたことが判明したことから更に調査を進めたところ、当該サーバーから何らかのデータの一部が社外に流出した可能性があることが確認されました。

なお、現時点で防衛や原子力に関する保護すべき情報が社外へ流出したことは確認されておりません。その他製品についても、引き続き調査をしております。

お客様及び関係先には多大なご心配とご迷惑をおかけしたことをお詫び申し上げるとともに、今後とも引き続き調査を進め、警察の捜査に全面的に協力して参ります。

以上