平成 20 年 10 月 10 日

NEWS RELEASE

www.jogmec.go.jp

独立行政法人　石油天然ガス・金属鉱物資源機構

問合せ先:セキュリティ対策チーム
TEL:044-520-8810
（お問合せ時間　平日9:00～18:00）

JOGMEC 公開サーバーに対する不正侵入とホームページの改ざんについて

（続報）

JOGMEC の公開サーバーに対する不正侵入が発生し、ホームページの改ざんが行われたことについては、平成 20 年 9 月 18 日にホームページに『JOGMEC 公開サーバーに対する不正侵入とホームページの改ざんについて』を発表しております。

今般、セキュリティ対策専門会社と共に行ってきた改ざん内容、被害状況等の調査結果が以下の通り判明しましたので、お知らせ致します。

（１） 不正アクセスの手法と内容

平成 20 年 7 月 27 日夜、JOGMEC の外部公開サーバーの一つである、下記（２）①法人文書ファイル検索サービスサーバーに SQL インジェクションにより不正侵入が行われました。

その後、同様な手口にて下記（２）②、③、④のサーバーでプログラムの改ざん等が行われました。

（２） 改ざんが行われたウェブサイトと被害内容

① 法人文書ファイルの検索サービスサイト
http://inf.jogmec.go.jp/

② バーチャル金属資源情報センターのデータベース検索サービスサイト
http://mric.jogmec.go.jp/tango/result.asp
http://mric.jogmec.go.jp/current/08_56.html
http://mric.jogmec.go.jp/gims/
http://mric.jogmec.go.jp/gims/login.html
http://mric.jogmec.go.jp/shigen_hp.asp
http://mric.jogmec.go.jp/shigen_hp1.asp

③ JOGMEC 英文ホームページにおけるお問い合わせサービスサイト
http://www.jogmec.go.jp/english/contact/

④ 休廃止鉱山情報検索サービスサイト
（一般へのサービスは行っておりません）

① については、プログラムの書換えが判明したものの、有害なサイトに強制的に誘導されることは確認されておりません。

② の http://mric.jogmec.go.jp/tango/result.asp については、鉱業・鉱物資源用語集の用語検索サービスを行うプログラムの書換えが、他のサイトについては、検索結果を表示させるプログラムの書換えが判明しました。この書換えられたプログラムにより有害なサイトに強制的に誘導され、悪性プログラム(ウィルス)のインストールが行なわれることが確認されました。

③ については、当方の認知していないプログラムが置かれたことが判明しましたが、このプログラムにより有害なサイトに強制的に誘導されることは確認されておりません。

④ については、プログラムの書換えが判明しました。この書換えられたプログラムにより、本サイトにアクセスしただけで②と同じ有害なサイトに強制的に誘導され、悪性プログラム(ウィルス)のインストールが行なわれることが確認されました。

（３） 外部における被害

②及び④のサイトへのアクセス、又は用語検索サービスを利用された方のパソコンが悪性プログラム(ウィルス)に感染した恐れがあります。

（４） 対応策

上記（３）により感染したことが確認されている以下のウィルスについては、トレンドマイクロ社のウィルス対策ソフト(2008 年 9 月 17 日以降に配布されたパターンファイル 5.549.00）により、検知、駆除されることが確認されておりますので、パターンファイルを更新の上、スキャンされることをお薦め致します。尚、トレンドマイクロ社のウェブサイトでは、以下のウィルスを検知、駆除する無料のオンラインスキャンサービスも提供されております。

（ http://www.trendflexsecurity.jp/security_solutions/housecall_free_scan.php?Homeclick=threat_onlinescan#）

トレンドマイクロでの検知名	種類
BKDR_AGENT.AKMI	バックドア型
TROJ_AGENT.IUK	トロイの木馬型
BKDR_BLAZGEL.I	バックドア型
TSPY_AGENT.ISN	トロイの木馬型
TROJ_AGENT.GUO	トロイの木馬型
TROJ_FAKEGINA.AB	トロイの木馬型

（５） 今後の対応

JOGMEC としては、公開サーバーのセキュリティを一層強固にすべく必要な作業を行っておりますので一部の外部サービスを暫くの間、停止させて頂くことをご了解下さい。JOGMEC の情報提供サービスを利用されている皆様にご迷惑をおかけ致しましたこと及び当面のサービス停止につき、深くお詫び申し上げます。

以　上