青い森のサイバーセキュリティ

令和４年３月
青森県警察本部保安課
サイバー犯罪対策室

緊急性の高い「Apache Log4j」の脆弱性

ネット上に公開されたサーバが不正侵入を受ける危険性

昨年11月24日以降、NISC(内閣官房サイバーセキュリティセンター）を初めとした各セキュリティ専門機関から、「Apache Log4j(アパッチ ログ フォー ジェイ)」の脆弱性についての注意喚起がなされていますが、これはどのようなものなのでしょうか。

今回の「Apache Log4j」の脆弱性とは、「Log4jが使用されているシステムに外部から特定の文字列を【システムログ】に記録するよう仕向けると、**システムが勝手に外部と通信してしまう**」というものです。

これで何が起きるかというと、悪意のある人物が外部からの操作で公開サーバを**容易に乗っ取る**ことが出来、自由にウイルス感染や情報漏洩をさせることが出来るようになってしまいます。

「Log4j」はプログラミング言語「Java」を使用したシステムにおけるメジャーなログ記録ライブラリで、公開サーバの構築においては「Java」と「Log4j」の組み合わせはよく使われています。

公開システムを運用している企業・団体の方は、必ずシステムに「Java」が使われていないか、使われていれば脆弱性のあるバージョンの「Log4j」が使われていないか、を確認していただくよう御願いします。

県内でEmotet類似のメールの受信が増えています

これまでにも何度かお知らせしておりますが、ここ数週間、青森県内のメールアドレス宛に、拡張子が「.xls」や「.zip」のEmotet系のウイルスが添付されたメール（リンクのみが張られたものも含む。）が多量に送信されているようです。

送信元は海外のサーバの様ですが、ファイルを開くとウイルスに感染する可能性がありますので、不用意に添付ファイルやリンクを開かないでください。

Attached is an important Excel document: 2460_130372398.xls

Thank you,

取引相手等の名前
（注：実際の送信者とは異なります）

Hi

Please see/review attached.
Thanks

doc 406955.zip

archive password - 972

Thank you,

実際に送信されたメール（一部加工してあります）