

## LicenseGuard、及びPCヘルスチェッカーにおける「アプリケーションディレクトリ型DLL問題」に起因する脆弱性対応について

ご使用頂いております「License Guard」(以下、LG)、及び「PCヘルスチェッカー」(以下、PCH)製品における「DLL読み込み問題」への対応について下記に記載致します。

### 1. DLL 読み込み問題

DLL 読み込み問題とは、Windows 環境でアプリケーションが本来読み込むべきではない DLL ファイルを読み込む状況が発生することに起因する問題です。例えば、以下の手順で発生します。

- (1) ダウンロードなどによって、不正な DLL ファイルを PC 内に持ち込んでしまう
- (2) 不正な DLL ファイルが保存されているフォルダに、実行ファイルを保存する(※1)
- (3) 実行ファイルを起動すると、不正な DLL ファイルを読み込んでしまう

※1: 例えば、Web ブラウザを用いてファイルをダウンロードすると、同一のフォルダに保存されます。

DLL 読み込み問題の詳細は、以下のサイトをご覧ください。

・HIRT-PUB17011: DLL 読み込み問題

<http://www.hitachi.co.jp/hirt/publications/hirt-pub17011>

・JVNTA#91240916 Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題

<https://jvn.jp/ta/JVNTA91240916/index.html>

DLL 読み込み問題には OS の動作に起因して発生するケースもあり、アプリケーション側だけでは対策できないケース(※2)があります。

※2: 「HIRT-PUB17011: DLL 読み込み問題」の「表 2: アプリケーションディレクトリ型 DLL 問題対策の分類」を参照

「LG」、及び「PCH」では、この「アプリケーションディレクトリ型 DLL 問題」に対する対応を実施しております。

### 2. DLL 読み込み問題の回避方法

以下のいずれかの方法で回避できます。

- ・新規に作成したフォルダに実行ファイルを移動してから起動する
- ・実行ファイルと同じフォルダに、不正な DLL ファイルなどがないことを確認してから起動する

### 3. 「LG」、及び「PCH」の対応

不正な DLL ファイルが PC 内に持ち込まれた環境で、LG、及び PCH のアプリケーション(実行ファイル)を同じフォルダに格納し実行すると、DLL ファイル内の任意のコードが実行されるケースを確認しています。

今回、DLL 読み込み問題が発生する可能性のあるアプリケーションを調査し、その調査結果と対策予定を以下の表 1 に示します。表 1 の対象は、いずれも DLL 読み込みを実施しているアプリケーションです。

そのうち、問題有無が「無」となっているアプリケーションはクライアントマシン上で認知済みとして登録されている DLL(※3)のみが呼び出されているため、本件に対しては問題ありません。

問題有無が「有」となっているアプリケーションは、認知済みとして登録されていない DLL が一部呼び出されているため、これらに対しては対策を推進致します。また、対策完了までの期間は「2. DLL 読み込み問題の回避方法」の実施をお願いします。

※3: KnownDLLs レジストリキーに登録済みの DLL(“既知の DLL”)を指します。これらの DLL は登録済みのパス情報に従って DLL が読み込まれます。

・Windows が使用する DLL 検索パス

<https://msdn.microsoft.com/ja-jp/library/7d83bc18.aspx>

表 1. DLL 読み込み問題が発生する可能性のある LG、及び PCH のアプリケーション

#	アプリケーション (実行ファイル)	製品 種別	問題 有無	問題点	対策予定
1	LGAgent	LG	有	クライアントからのサーバとの通信処理で、DLL 読み込み問題が発生する可能性がある	2018 年 3 月 31 日 リリース予定
2	自マシン情報収集 ツール	LG	無	-	対策不要
3	スタンドアロンマシン 情報収集ツール	LG	無	-	対策不要
4	スタンドアロンマシン 情報登録(Windows 2000 以前用)	LG	有	常時稼動における、サーバとの通信処理の際、DLL 読み込み問題が発生する可能性がある	2018 年 3 月 31 日 リリース予定
5	PC ヘルスチェッカー (クライアントツール)	PCH	有	ユーザセッションに関するセキュリティ情報の取得処理の際、DLL 読み込み問題が発生する可能性がある	2018 年 3 月 31 日 リリース予定

#### 4. お願い事項

対策版の提供まで、「2. DLL 読み込み問題の回避方法」での運用をお願いします。