CompuSec 製品のインストーラーにおける DLL 読み込みに関する

脆弱性への対応について

キヤノン IT ソリューションズ株式会社
公開日：2018 年 8 月 27 日

拝啓　貴社ますますご盛栄のこととお喜び申し上げます。
平素は CompuSec 製品につきまして格別のご高配を賜り、厚くお礼申し上げます。
CompuSec 製品の脆弱性への対応についてご案内します。

今回、新たに CompuSec インストーラーに含まれるランチャープログラム本体に DLL 読み込みに関する脆弱性が見つかりました。これから CompuSec 製品を新規にインストールするお客さまは、弊社 Web ページにて現在公開しております最新のインストーラーをダウンロードしてご利用くださいますようお願いします。すでにインストールが完了している場合には、この脆弱性の影響はありません。また、2018 年 8 月 27 日 15:00 より前にダウンロードされましたインストーラーは、速やかに削除し、ご利用にならないでください。
今回の脆弱性の詳細は以下のとおりで、更新された項目には、赤字の太字で記述しております。

※本内容は 2018 年 7 月 18 日に公開いたしました「CompuSec 製品のインストーラーにおける DLL 読み込みに関する脆弱性への対応について」とは異なる脆弱性への対応となります。

＜目次＞

1）脆弱性の対象となる CompuSec 製品・プログラム

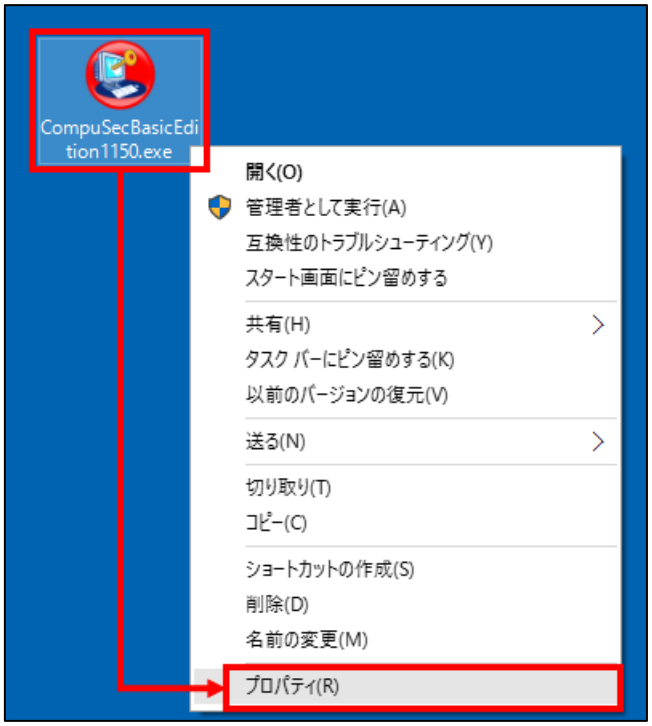
以下の製品で提供しているプログラムのインストーラー（**デジタル署名のタイムスタンプの日付が「2018年7 月30日」以前のもの**）が対象です。

◇ 個人向け製品
- CompuSec SW ダウンロード
- **CompuSec SW パッケージ**

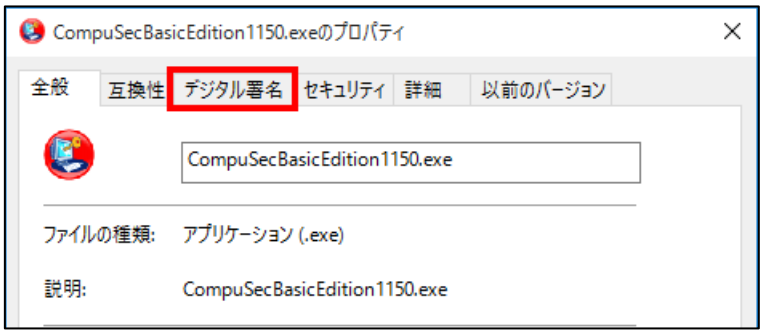
◇ 法人向け製品
- CompuSec Basic Edition
- CompuSec Standard Edition
- CompuSec SW ライセンス
- CompuSec Pro ライセンス

インストーラーのデジタル署名の確認方法

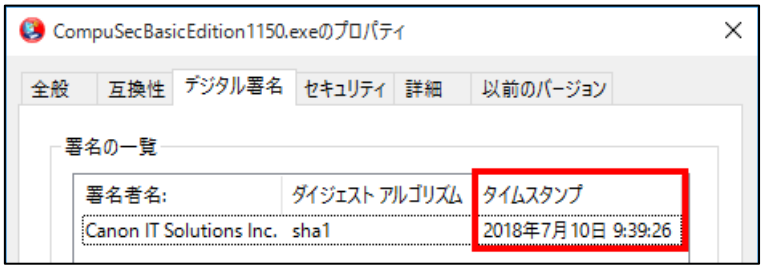
1. デスクトップなどに保存しているインストーラーを右クリックし「プロパティ」を選択します。



2. インストーラーのプロパティ画面が表示されるので、「デジタル署名」タブをクリックします。



3. 「タイムスタンプ」に表示されている日付を確認してください。



2）脆弱性の詳細情報

CompuSec インストールプログラム（自己解凍型アーカイブ）を解凍後、CompuSec のインストールを行うために、ランチャープログラム「csinstall(インストールはこちら).exe」を実行し、DLL が読み込まれる際の検索パスに問題があるため、ランチャープログラムと同一のディレクトリに存在する特定の DLL ファイルを読み込んでしまう脆弱性が存在します。

3）想定される影響

ランチャープログラムを実行している権限で、任意のコードが実行される可能性があります。

前回は、自己解凍型アーカイブである CompuSec インストールプログラムを実行し、アーカイブを解凍開始した時点で、脆弱性の影響を受けました。今回は CompuSec インストールプログラムが解凍され、ランチャープログラムである「csinstall(インストールはこちら).exe」が実行されたときに、脆弱性の影響を受けます。

なお、本脆弱性の影響を受けるのは「csinstall(インストールはこちら).exe」の起動時のみです。既にインストールが完了している CompuSec 製品は影響を受けません。

4）対応方法

2018 年 8 月 27 日 15:00 頃、本脆弱性を修正したインストーラーを公開しました。

これから CompuSec 製品をインストールするお客さまは、以下の Web ページにて現在公開しております最新のインストーラーをダウンロードしてご利用くださいますようお願いします。

2018 年 8 月 27 日 15:00 より前にダウンロードされましたインストーラーは、速やかに削除してください。

◇ 個人向け製品

CompuSec SW パッケージ

▼パッケージ版プログラムのダウンロードページ

http://canon-its.jp/product/cs/sw_upgrade.html

CompuSec SW ダウンロード

▼ダウンロード版プログラムの再ダウンロードページ

https://eset-info.canon-its.jp/support/wc0102/#CS

◇ 法人向け製品

CompuSec Basic Edition

CompuSec Standard Edition

CompuSec SW ライセンス

CompuSec Pro ライセンス

▼ライセンスユーザーさま専用ユーザーズサイト

https://canon-its.jp/cgi-bin/csuser_site_login.cgi

5）本件に関するお問い合わせ窓口

暗号化製品サポートセンター

https://www.canon-its.co.jp/products/compu_sec/support/detail/contact.html

お客さまにはご迷惑をお掛けしましたことを、深くお詫び申し上げます。

＜参考情報：2018 年 7 月 18 日にご案内していました内容につきまして＞

公開日：2018 年 7 月 18 日

これから CompuSec 製品をインストールするお客さまは、Web ページにて現在公開しております最新のインストーラーをダウンロードしてご利用くださいますようお願いします。
また、2018 年 7 月 18 日 10:00 より前にダウンロードされましたインストーラーは、速やかに削除してください。
※ パッケージ製品に同梱された CD-ROM を利用する場合は本脆弱性の影響はありません。

本脆弱性の詳細は以下のとおりです。

＜目次＞

1）脆弱性の対象となる CompuSec 製品・プログラム

以下の製品で提供しているプログラムのインストーラー（デジタル署名のタイムスタンプの日付が「2018年7 月10日」以前のもの）が対象です。

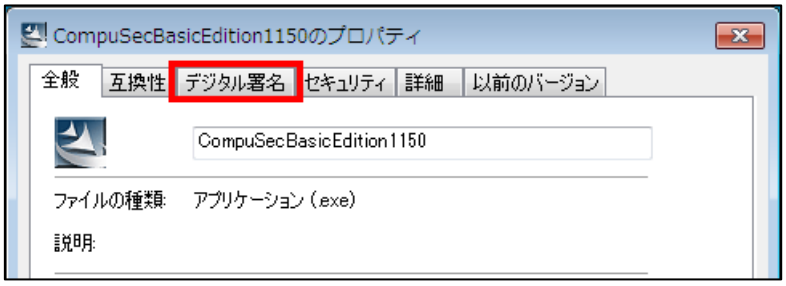
◇ 個人向け製品
CompuSec SW ダウンロード

◇ 法人向け製品
CompuSec Basic Edition
CompuSec Standard Edition
CompuSec SW ライセンス
CompuSec Pro ライセンス

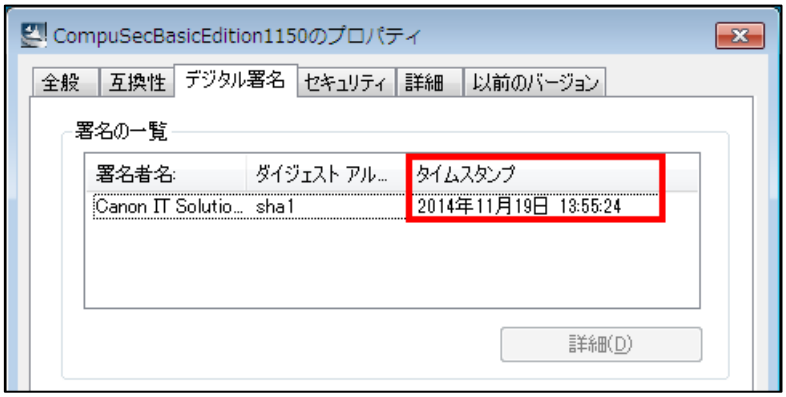
インストーラーのデジタル署名の確認方法

1. デスクトップなどに保存しているインストーラーを右クリックし「プロパティ」を選択します。

2. インストーラーのプロパティ画面が表示されるので、「デジタル署名」タブをクリックします。



3. 「タイムスタンプ」に表示されている日付を確認してください。



2）脆弱性の詳細情報

対象のインストーラーは、DLL を読み込む際の検索パスに問題があるため、インストーラーと同一のディレクトリに存在する特定の DLL ファイルを読み込んでしまう脆弱性が存在します。

3）想定される影響

インストーラーを実行している権限で、任意のコードが実行される可能性があります。
なお、本脆弱性の影響を受けるのはインストーラーの起動時のみです。既にインストールされた CompuSec 製品は影響を受けません。

4）対応方法

2018 年 7 月 18 日 10:00 頃、本脆弱性を修正したインストーラーを公開しました。
これから CompuSec 製品をインストールするお客さまは、以下の Web ページにて現在公開しております最新のインストーラーをダウンロードしてご利用くださいますようお願いします。
2018 年 7 月 18 日 10:00 より前にダウンロードされましたインストーラーは、速やかに削除してください。
※ パッケージ製品に同梱された CD-ROM を利用する場合は本脆弱性の影響は受けません。

◇ 個人向け製品

CompuSec SW ダウンロード

▼ダウンロード版プログラムの再ダウンロードページ

https://eset-info.canon-its.jp/support/wc0102/#CS

◇ 法人向け製品

CompuSec Basic Edition
CompuSec Standard Edition
CompuSec SW ライセンス
CompuSec Pro ライセンス

▼ライセンスユーザーさま専用ユーザーズサイト

https://canon-its.jp/cgi-bin/csuser_site_login.cgi

5）本件に関するお問い合わせ窓口

暗号化製品サポートセンター
https://www.canon-its.co.jp/products/compu_sec/support/detail/contact.html

お客さまにはご迷惑をお掛けしましたことを、深くお詫び申し上げます。