

XCC Event Logger

ユーザーズマニュアル

2024 年 3 月
セイ・テクノロジーズ株式会社

免責事項

本稿に記載された内容は、予告無しに変更される場合があります。

セイ・テクノロジーズ株式会社は、本稿に関していかなる種類の保証（商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません）もいたしません。

セイ・テクノロジーズ株式会社は、本稿に含まれた誤謬に関しての責任や、本稿の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。

本稿の内容は 2024 年 3 月時点で行った検証に基づいており、お客様がご利用する際には最新情報をご確認ください。

目次

1. XCC Event Logger について	1
1.1. 動作環境	1
1.2. システム構成	1
2. インストール・アンインストール	2
2.1. XCC Event Logger の新規インストール方法について	2
2.2. XCC Event Logger のアップグレード方法について	5
2.3. XCC Event Logger のアンインストール方法について	6
2.4. ユーザーID の変更方法について	6
3. 設定ファイル	7
3.1. 設定ファイルについて	7
3.1.1. 接続情報設定ファイル(server.yml)	8
3.1.2. コマンド設定ファイル(command.yml)	9
3.1.3. ログ設定ファイル(log.yml)	10
3.2. イベントログへ書き込む際のフォーマットについて	11
4. XCC Event Logger の開始・停止	12
4.1. XCC Event Logger の開始	12
4.2. XCC Event Logger の停止	12
5. 付録	13
5.1. YAML フォーマットについて	13
5.1.1. YAML フォーマットとは	13
5.1.2. 基本的な記載方法	13
5.1.3. 正規表現の特殊記号を含める場合の記載方法	15

1. XCC Event Logger について

XCC Event Logger は、ThinkSystem サーバー内蔵型のシステム管理プロセッサ（X-Clarity Controller、以降 XCC と呼ぶ）へ一定間隔で接続し、XCC のログ採取を行い Windows イベントログへ出力を行うサービスです。

本項では XCC Event Logger の概要についてご紹介していきます。

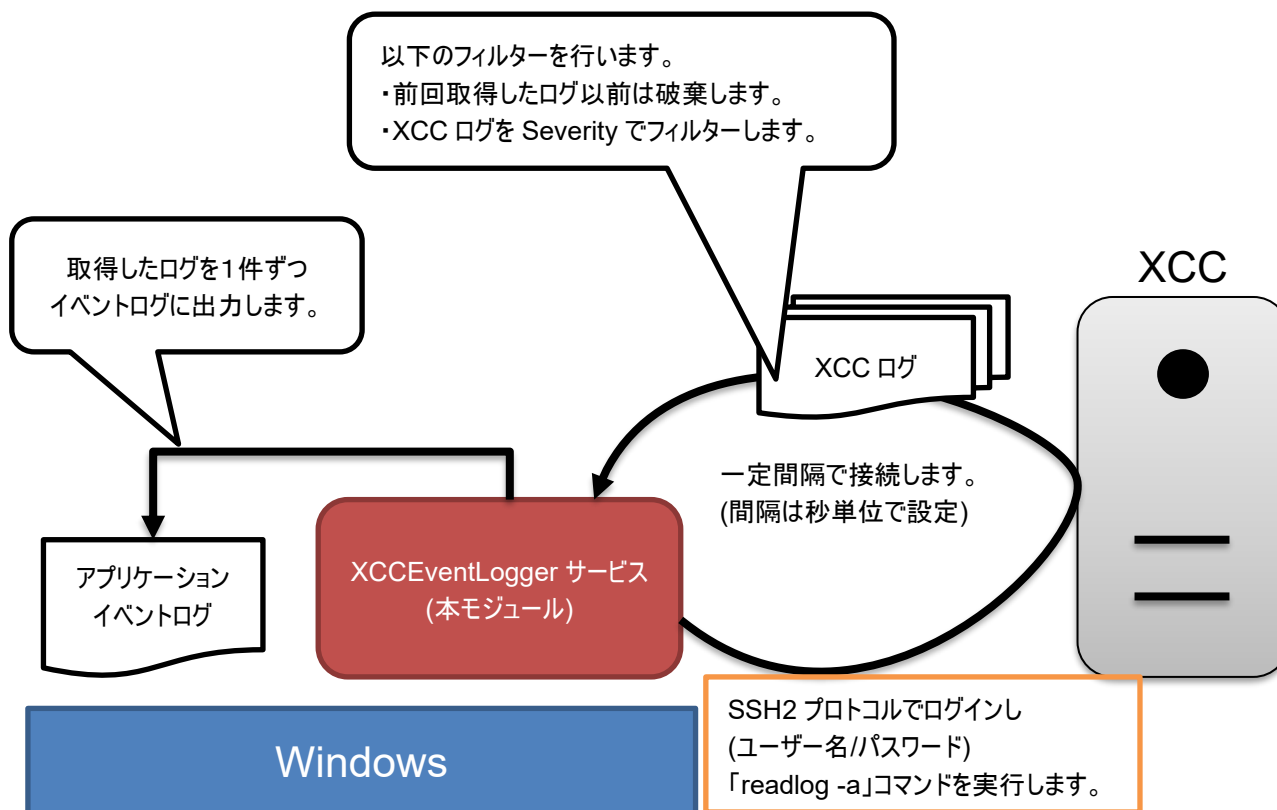
1.1. 動作環境

動作環境の最新情報については、以下の URL をご参照下さい。

URL: <https://www.say-tech.co.jp/product/xcceventlogger/req>

1.2. システム構成

システム構成と動作概要は以下の通りです。

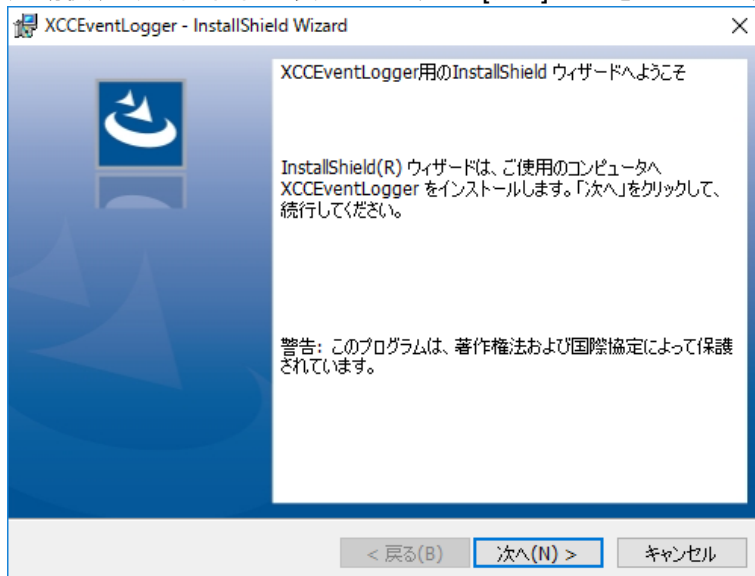


2. インストール・アンインストール

2.1.XCC Event Logger の新規インストール方法について

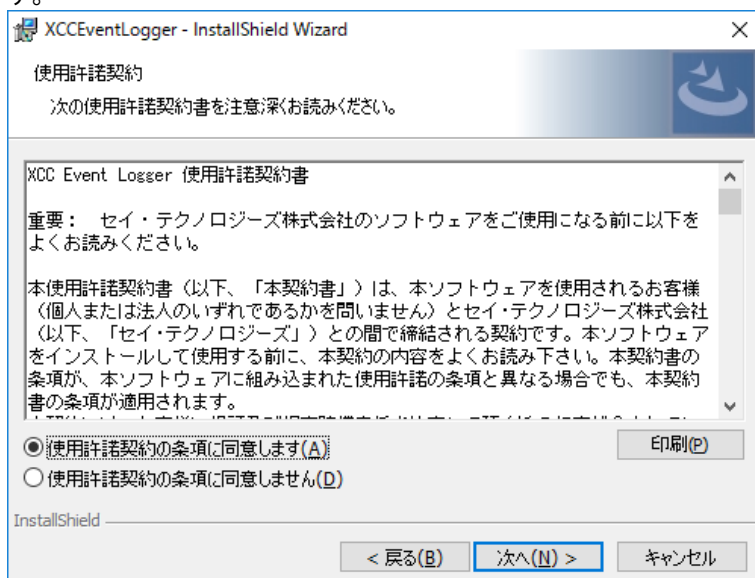
XCC Event Logger の新規インストール手順についてご案内いたします。

1. 管理者権限で Windows にログインします。
2. Setup.exe を起動します。
3. 起動後、ようこそ画面が表示されますので[次へ]ボタンをクリックします。



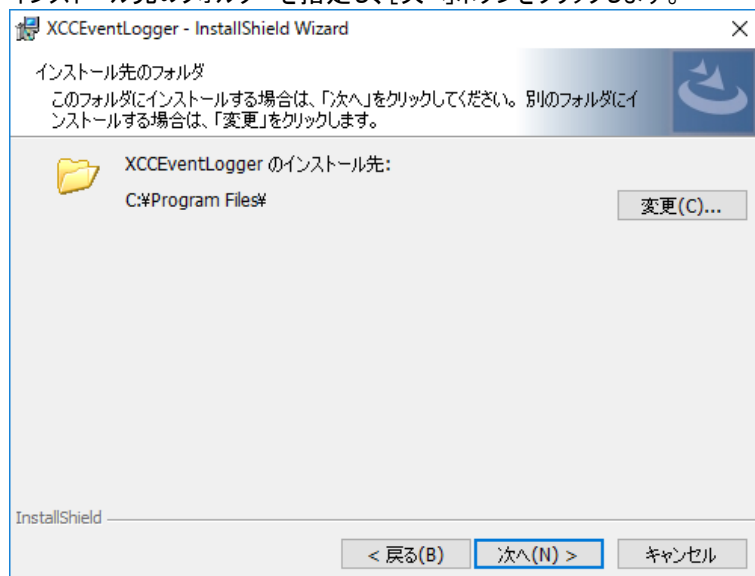
a. ようこそ画面

4. 使用許諾契約の画面が表示されますので、[使用許諾の条項に同意します]を選択し、[次へ]ボタンをクリックします。



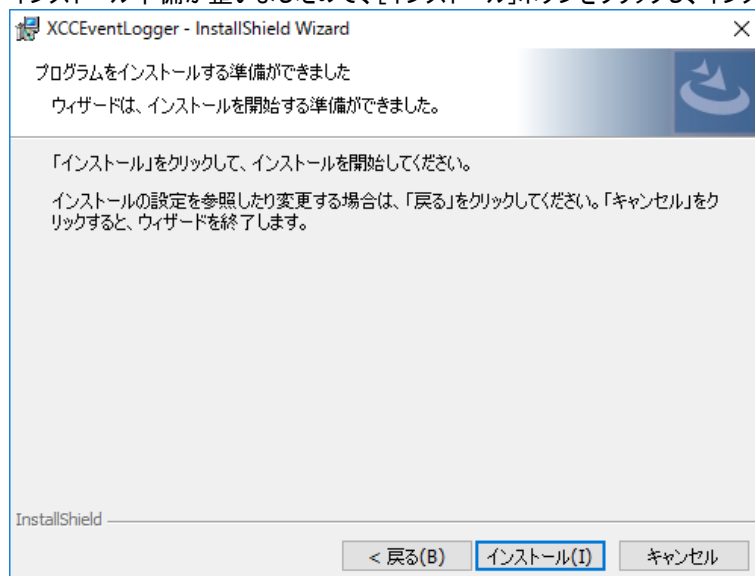
b. 使用許諾契約の画面

5. インストール先のフォルダーを指定し、[次へ]ボタンをクリックします。



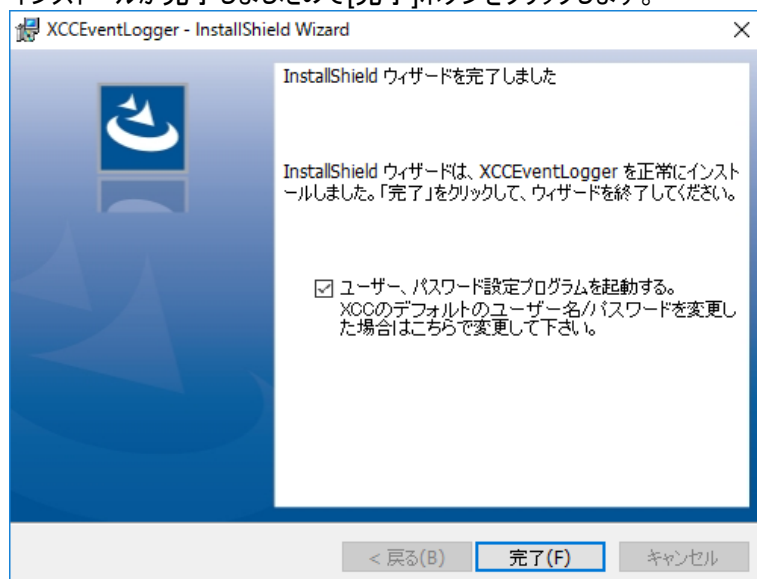
- c. インストール先フォルダー指定の画面

6. インストール準備が整いましたので、[インストール]ボタンをクリックし、インストールを開始します。



- d. インストール準備完了の画面

7. インストールが完了しましたので[完了]ボタンをクリックします。

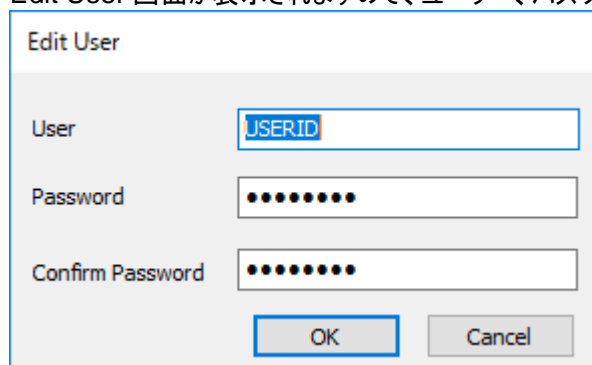


e. インストール完了の画面

※インストール完了時に"e. インストール完了の画面"内のチェックボタンをチェックすると、ユーザー登録変更画面 ("Edit User")が表示されます。チェックを外し、ユーザー変更を省略した際の初期設定値は以下のとおりです。

項目名	設定値
User	USERID
Password	PASSW0RD (0 は数字のゼロ)

8. Edit User 画面が表示されますので、ユーザー、パスワードを変更し、[OK]ボタンをクリックします。



f. Edit User 画面

※登録するユーザーとパスワードは XCC でユーザー作成後、必ず XCC にログインし、パスワード変更後のユーザーとパスワードを設定ください。XCC にアカウント作成後、XCC にログインせず、本設定を行った場合には動作しませんのでご注意ください。

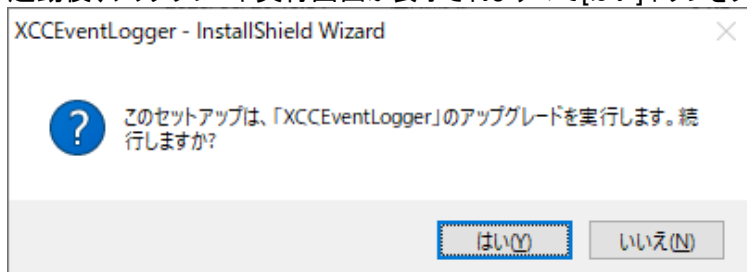
本インストールにより、以下のサービスが Windows のサービスに追加されます。

項目	内容
サービス名	XCCEventLogger
表示名	XCCEventLogger
スタートアップの種類	自動起動
依存関係	なし
サービスアカウント	ローカルシステムアカウント

2.2.XCC Event Logger のアップグレード方法について

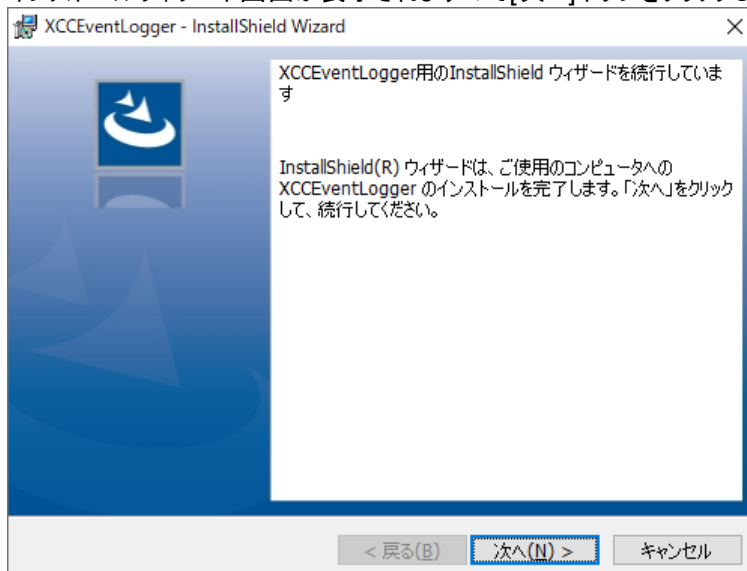
XCC Event Logger をすでにインストールしており、最新バージョンにアップグレードする手順についてご案内いたします。

1. 管理者権限で Windows にログインします。
2. Setup.exe を起動します。
3. 起動後、アップグレード実行画面が表示されますので[はい]ボタンをクリックします。



g. アップグレード実行画面

4. インストールウィザード画面が表示されますので[次へ]ボタンをクリックします。



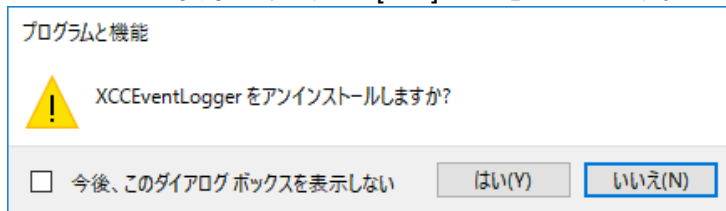
h. インストールウィザードの画面

インストールされた XCCEventLogger のバージョンは Windows の“スタート”から“コントロールパネル”を選択し、“プログラムのアンインストール”を選択します。登録された“XCCEventLogger”の“バージョン”で確認できます。

2.3.XCC Event Logger のアンインストール方法について

XCC Event Logger のアンインストール手順についてご案内いたします。

1. 管理者権限で Windows にログインします。
2. Windows の“スタート”から“コントロールパネル”を選択します。
3. “コントロールパネル”から“プログラムのアンインストール”を選択します。
4. プログラム一覧から“XCCEventLogger”を選択後、[アンインストール]ボタンをクリックします。
5. アンインストール要求が来ますので[はい]ボタンをクリックします。



i アンインストール確認要求画面

6. プログラムの一覧から“XCCEventLogger”が削除されていることを確認してください。

※アンインストール時に、イベントログビューアーを開いていると、使用中のファイルがある旨のメッセージが表示されます。その場合にはイベントログビューアーを終了して再度アンインストールを実行ください。

2.4.ユーザーID の変更方法について

ユーザーとパスワードを再設定するには、XCC Event Logger のアンインストール後、再度インストールする必要があります。

3. 設定ファイル

3.1. 設定ファイルについて

XCC からのアラートを受信するためには、接続情報設定ファイル及び、コマンド設定ファイルを設定する必要があります。設定ファイルのファイルフォーマット形式は YAML 形式 (Ver.1.2) です。

設定ファイルが格納されている場所は、以下の通りです。

➤ (インストールパス)¥XCCEVENTLOGGER¥conf

なお、各種設定ファイルは設定ファイルのファイルフォーマット形式は YAML 形式 (Ver.1.2) です。

※設定ファイルの変更は管理者権限でログインして実施ください。

※同一ユーザー、同一エンジン ID で複数行設定されている場合には、一番下の行に記載されている設定が適用されます。

※各設定ファイルの変更は、XCCEventLogger サービスの停止後に実施してください。設定内容の反映は XCCEventLogger サービス再起動後に行われます。

設定ファイル名	概要
server.yml	XCC 接続のための設定です。
command.yml	Windows イベントログに書き込む XCC のイベントログを指定できます。
log.yml	XCC Event Logger の動作ログの設定を指定できます。

3.1.1.接続情報設定ファイル(server.yml)

XCC へ接続するための情報を保持するファイルです。初期で設定されている値は以下の通りです。

```
server: 169.254.95.118
port: 22
user: USERID
password: hG/rdziZRf5JzDA3T4XW3g==
intervalSec: 600
```

既定値の接続先はローカルマシン、ポート:22、ユーザーID:USERID、パスワード:PASSWORD です。
実行周期は 10 分です。

項目	内容	必須	制限	詳細
Server	接続先 ホスト	○	1～255 文字	接続先ホスト (ipv4 or ipv6 or ホスト名)
port	ポート番号	○	0～65535 数値のみ	ポート番号
user	ユーザー名	○	1～32 文字	ユーザー名
password	パスワード(暗号)	△	サービス側で暗号化処 理が動作します	パスワード(暗号化) サービス側で暗号化する為変更 しないでください
passwordplain	パスワード(平文)	△	1～255 文字	パスワード(平文)
intervalSec	実行周期	○	5～31536000 数値のみ	実行周期(実行完了後、次回実 行するまでの待ち時間)

※password、passwordplain 両方指定されていた場合は、passwordplain が優先されます。

3.1.2.コマンド設定ファイル(command.yml)

XCC に対して送信コマンドとフィルター情報等を保持するファイルです。
初期設定は以下の通りです。

```
-
  command: readlog -a
# white_filters:
# -
black_filters:
  #ログインログは取得しない
  - 'Remote Login Successful%'
options:
  severity: I,W,E
  NoCheckTitle: true
# title: "Index,Severity,Service State,Source,Date,Sequence #,Event ID,Message,AuxLog"
```

項目	内容	必須	制限	詳細
command	実行コマンド	○	長さ: 1～4096	実行するコマンドを引数込みで記述します。
white_filters	ホワイトフィルター	×	長さ: 0～4096 配列数:256	ホワイトフィルター。 正規表現文字列で指定します。 コマンド実行結果に指定された文言が含まれていた場合はイベントログに出力します。 なお、指定がない場合は一致したとみなします。 デフォルトは指定していません。
black_filters	ブラックフィルター	×	長さ: 0～4096 配列数:256	ブラックフィルター。 正規表現文字列で指定します。 コマンド実行結果に指定された文言が含まれていた場合はイベントログに出力しません。 指定がない場合は一致していないとみなします。 デフォルトは指定していません。
options		×		コマンド毎に必要なキーと値を設定します。
severity	出力 severity	×	長さ: 0～4096(カンマ含む)	出力する severity を指定します。
IsNoCheckTitle	タイトルチェックするかどうか	×	True:チェックしない True 以外:チェックする	「readlog -a」を実行した時にタイトルチェックを行いません。
title	タイトル	×		「readlog -a」を実行した時チェックするタイトル。一致していないとエラーになります。

※正規表現は ECMAScript 互換です。

<https://msdn.microsoft.com/ja-jp/library/bb982727.aspx>

※ホワイトフィルターとブラックフィルター両方指定されていた場合は、ホワイトフィルターに一致かつブラックフィルターに一致しないものがイベントログに出力されます。

※ホワイトフィルターとブラックフィルターは設定ファイルに記載された順に評価され、一致した時点で以降のフィルターは無視されます。

※ブラックフィルターは既定の設定で SSH のログイン情報を設定しています。Windows イベントログには SSH のログイン情報は含まれません。もし、必要な場合には、- 'Remote Login Successful¥.'を削除するか、行頭に # を記述してください。

3.1.3.ログ設定ファイル(log.yml)

XCC Event Logger の動作ログファイルの設定を保持するファイルです。

```
file: ../logs¥log
num: 7
queueSiz: 32768
siz: 10485760
level: info
```

項目	必須	制限	内容
file	○	長さ: 1~250	ログ出力先パス
num	○	0~99	ローテーション数
queueSiz	○	2~32768 2 の累乗数	キューサイズ
siz	○	1~18,446,744,073,709,551,615	1 ファイル辺りのバイトサイズ
level	○	設定できる文字列以外は反映されません	ログ出力するログレベル。 以下の文字列が指定できます。
			高 ↑ critical error warning info ↑ debug 低 trace

※ログファイルの既定保存先は、以下の通りです。

(インストールパス)¥XCCEVENTLOGGER¥logs¥log

※ファイルサイズが 10MB になればファイル名を変更し、最大 7 つまでファイルを作成し、それ以降は最古ファイルを上書きします。

3.2. イベントログへ書き込む際のフォーマットについて

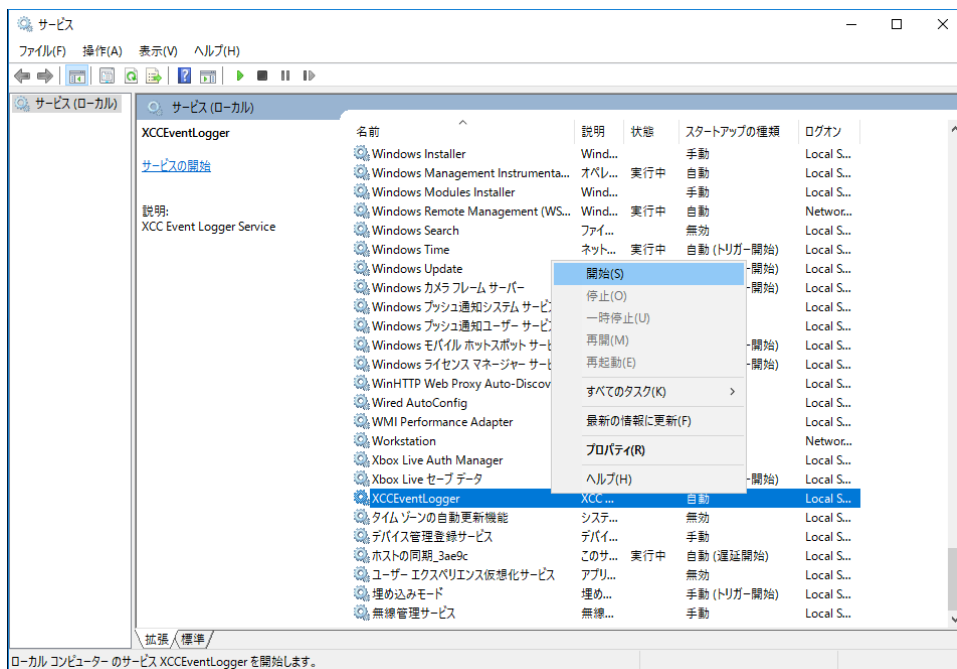
Windows のイベントログへ書き込まれる内容は以下の通りです。

項目	内容
ログの名前	Application
ソース	XCCEventLogger
メッセージ	
イベント ID	
レベル	
ユーザー	N/A
オペコード	- (空欄)
ログの日付	書き込み日時
タスクのカテゴリ	なし
キーワード	クラシック
コンピューター	XCCEventLogger サービスが動作しているコンピューター名

4. XCC Event Logger の開始・停止

4.1.XCC Event Logger の開始

XCC Event Logger を開始するには、Windows のサービスから XCC Event Logger を開始します。
XCCEventLogger サービスを開始してください。
※本操作は管理者権限で Windows にログインして実行ください。



j. サービス一覧

4.2.XCC Event Logger の停止

XCC Event Logger を停止するには、Windows のサービスから XCC Event Logger を停止します。
XCCEventLogger サービスを停止してください。
※本操作は管理者権限で Windows にログインして実行ください。

5. 付録

5.1. YAML フォーマットについて

5.1.1. YAML フォーマットとは

YAML フォーマットとは構造化されたデータを表現するためのフォーマットです。

- 公式サイト
<http://yaml.org/>

5.1.2. 基本的な記載方法

(ア) 配列

行頭に「-」をつけることで配列を表現します。「-」の後には半角スペースを入れます。

```
- aaa  
- bbb  
- ccc
```

(イ) ハッシュ

ハッシュは「キー: 値」の形式で表現します。「:」(コロン)の後に半角スペースを 1 つ以上入れます。(タブは使えません)

```
server: 169.254.95.118  
port: 22  
user: USERID
```

(ウ) 配列とハッシュのネスト

配列とハッシュはお互いにネストさせることができます。

配列の中にハッシュをネストさせる場合には、先頭にスペースを追加する必要があります。

```
-  
  company: say-tech  
  address: bunkyoku  
-  
  company: lenovo  
  address: chiyodaku
```


(エ) コメント

コメントは「#」です。「#」から行末までがコメントとして表示されます。

```
-
  #コメント行
  company: say-tech #ここからコメント
  address: bunkyoku
-
  company: lenovo
  address: chiyodaku
```

(オ) データ型

型	表記方法	内容	備考
数値	123	整数(10 進数)	
文字列その 1	'123'	文字列 シングルクォートで囲みます。	シングルクォート (') で囲まれた文字列のなかでシングルクォートをあらわすには、シングルクォートを 2 つ連ねます。
文字列その 2	"123"	文字列 ダブルクォートで囲みます。	以下の文字を含める場合は、「¥」(日本語 OS の場合。英語 OS はバックスラッシュ)でエスケープする必要があります。
文字列その 3	123	文字列 文字列型では文字列として扱われます。	

設定ファイルの記載	実際の内容
- "ABC :{}[],&*#? -<>=!%@"¥" 123"	ABC :{}[],&*#? -<>=!%@"¥" 123
- 'ABC :{}[],&*#? -<>=!%@"¥" 123'	ABC :{}[],&*#? -<>=!%@"¥" 123
- ABC :{}[],&*#? -<>=!%@"¥" 123	ABC :{}[],&*#? -<>=!%@"¥" 123

5.1.3.正規表現の特殊記号を含める場合の記載方法

“3.1.2 コマンド設定ファイル(command.yml)”のホワイトフィルター、ブラックフィルターで正規表現の特殊記号を文字として認識させたい場合には「¥」でエスケープする必要があります。

エスケープ前	エスケープ後
¥	¥¥
*	¥*
+	¥+
.	¥.
?	¥?
{ }	¥{ ¥}
()	¥(¥)
[]	¥[¥]
^	¥^
\$	¥\$
-	¥-
	¥
/	¥/
*	¥*
+	¥+
.	¥.
?	¥?
{ }	¥{ ¥}

XCC Event Logger ユーザーズマニュアル

2017 年 11 月 17 日 初版
2024 年 3 月 15 日 改訂版

著者 セイ・テクノロジーズ株式会社
発行者 セイ・テクノロジーズ株式会社
発行 セイ・テクノロジーズ株式会社

© 2017-2024 SAY Technologies, Inc.