

SureServer[SHA-2]証明書の仕様変更について

サイバートラスト株式会社
2017年03月05日

■ 変更内容

■ サーバー証明書の特長領域

- 「basicConstraints (基本制限)」を「non-critical」から「critical」に変更
- 「certificatePolicies(証明書ポリシー)」にOID「2.23.140.1.2.2」を追加

■ 対象

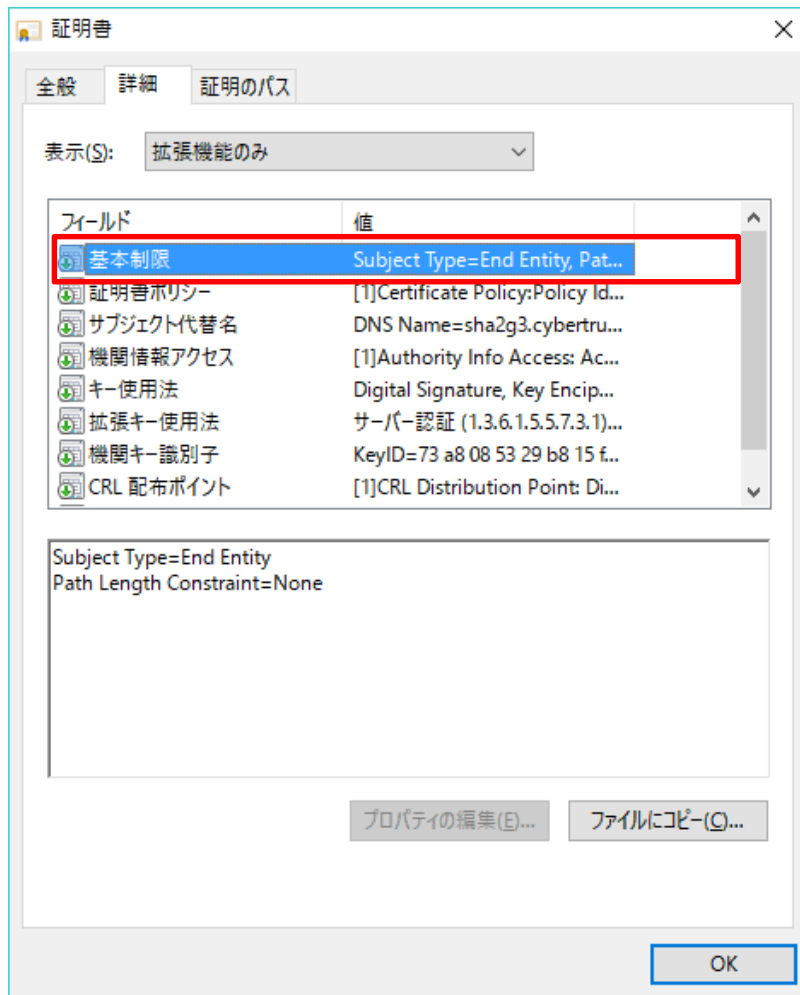
- 2017 年 3 月 5 日（日）以降に発行された
SureServer [SHA-2]証明書 (MD/クラウド商品を含む)

■ 対応・影響

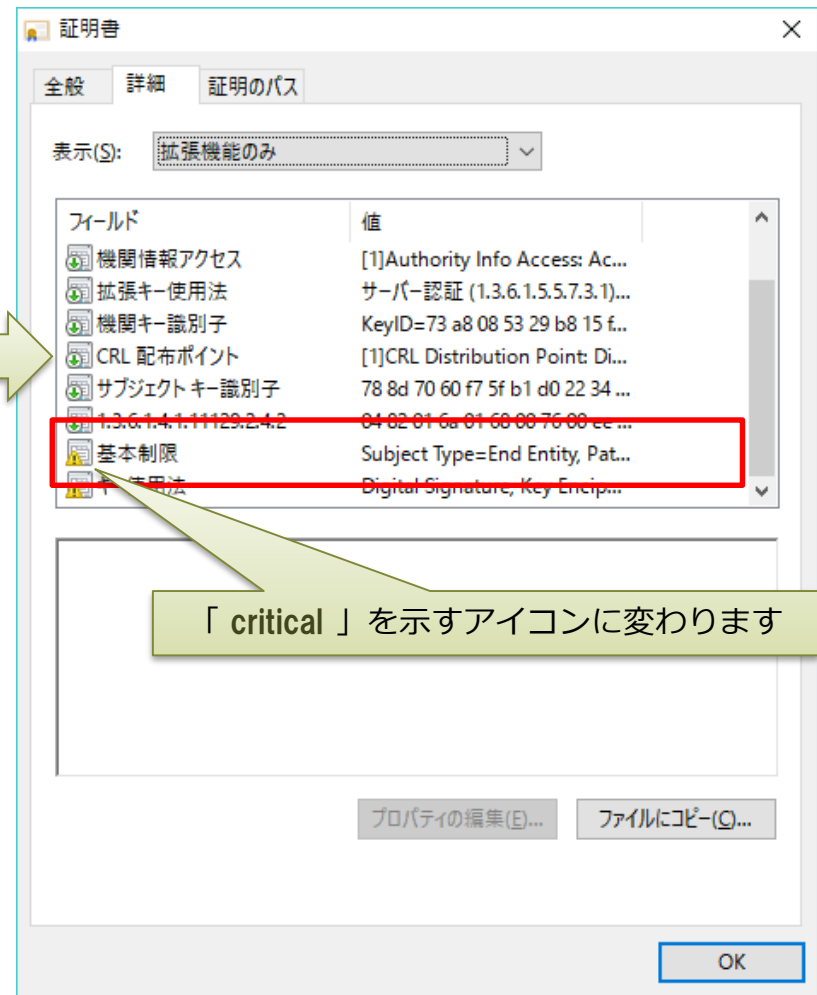
- 発行済みのサーバー証明書に影響はなく、**お客様のご対応は不要**です。
- Webブラウザ、モバイルカバー率に影響はなく、従来と同じ対応率でご利用いただけます。

2. 仕様変更後の証明書 1/2

■ 変更前

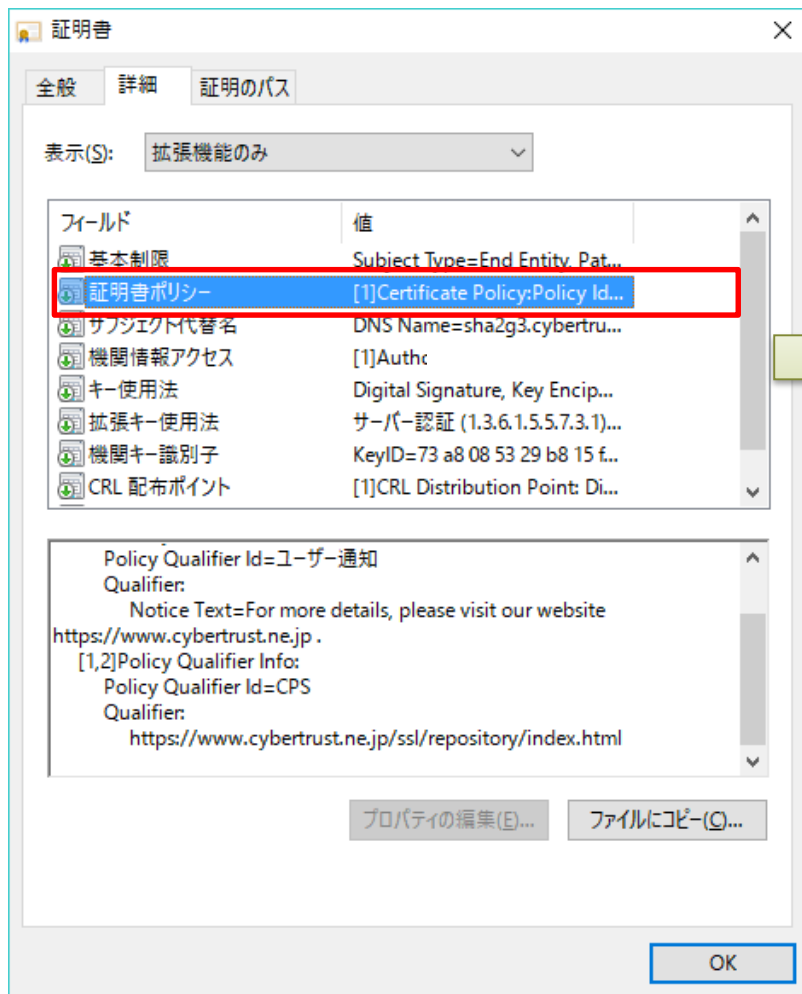


■ 変更後



2. 仕様変更後の証明書 2/2

■ 変更前



証明書

全般 詳細 証明のパス

表示(S): 拡張機能のみ

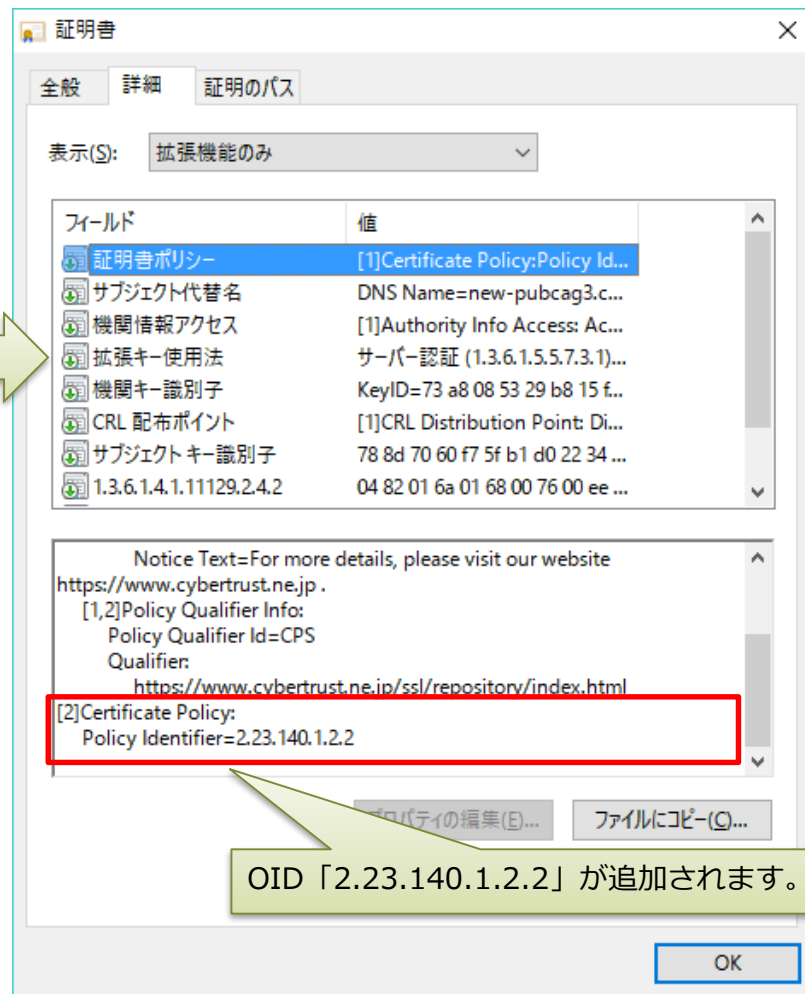
フィールド	値
基本制限	Subject Type=End Entity, Pat...
証明書ポリシー	[1]Certificate Policy:Policy Id...
サブジェクト代替名	DNS Name=sha2g3.cybertru...
機関情報アクセス	[1]Authc
キー使用法	Digital Signature, Key Encip...
拡張キー使用法	サーバー認証 (1.3.6.1.5.5.7.3.1)...
機関キー識別子	KeyID=73 a8 08 53 29 b8 15 f...
CRL 配布ポイント	[1]CRL Distribution Point: Di...

Policy Qualifier Id=ユーザー通知
Qualifier:
Notice Text=For more details, please visit our website
<https://www.cybertrust.ne.jp> .
[1,2]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
<https://www.cybertrust.ne.jp/ssl/repository/index.html>

プロパティの編集(E)... ファイルにコピー(C)...

OK

■ 変更後



証明書

全般 詳細 証明のパス

表示(S): 拡張機能のみ

フィールド	値
証明書ポリシー	[1]Certificate Policy:Policy Id...
サブジェクト代替名	DNS Name=new-pubcag3.c...
機関情報アクセス	[1]Authority Info Access: Ac...
拡張キー使用法	サーバー認証 (1.3.6.1.5.5.7.3.1)...
機関キー識別子	KeyID=73 a8 08 53 29 b8 15 f...
CRL 配布ポイント	[1]CRL Distribution Point: Di...
サブジェクト キー識別子	78 8d 70 60 f7 5f b1 d0 22 34 ...
1.3.6.1.4.1.11129.2.4.2	04 82 01 6a 01 68 00 76 00 ee ...

Notice Text=For more details, please visit our website
<https://www.cybertrust.ne.jp> .
[1,2]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
<https://www.cybertrust.ne.jp/ssl/repository/index.html>
[2]Certificate Policy:
Policy Identifier=2.23.140.1.2.2

プロパティの編集(E)... ファイルにコピー(C)...

OK

OID「2.23.140.1.2.2」が追加されます。

Q. basicConstraints (基本制限)とは？

A. basicConstraints (基本制限)は、以下の2点について制限するものです。

- 証明書がCAであるか否か
- 証明書を含む有効な最深の証明書階層

Q. OID「2.23.140.1.2.2」とは？

A. CA/ブラウザフォーラムが定める「企業認証（OV）」の区分を表す共通の値です。

Q. なぜ仕様変更をするのでしょうか？

A. Omnirootの移管に伴い、Digicert社の仕様と合わせるためです。



<https://www.cybertrust.ne.jp>

詳細は下記まで、お問い合わせください。

0120-957-975

電話受付時間 平日 9:00 ~ 18:00

✉ servicedesk@cybertrust.ne.jp