群馬県立学校 ICT 環境整備業務

BYOD 接続手順

Windows 11

Ver. 0.1

令和 4 年 10 月 20 日作成

目次

1.	はじ	こと こう	. 2
1	1.1.	本書の目的	2
2.	接緩	長手順	. 3
2	2.1.	BYOD 向け無線 LAN 用証明書のインストール	4
2	2.2.	プロキシサービス用 SSL 証明書のインストール	8
2	2.3.	BYOD 向け無線 LAN 接続実施	13
2	2.4.	プロキシ設定確認	16
2	2.5.	Web アクセス実施、プロキシサービスヘログイン	18
3.	証明]書削除手順	21
ê	3.1.	プロキシサービス用 SSL 証明書の削除	21
ć	3.2.	BYOD 向け無線 LAN 用証明書の削除	27

1. はじめに

1.1. 本書の目的

本書は、Windows 11の持ち込み端末(BYOD)における学校利用に必要な接続手順を記載します。

2. 接続手順

BYOD 端末接続時の手順について説明します。接続手順のイメージは下図の通りとなります。



*1 p12 ファイルとは、パスワードに基づく鍵(暗号)により保護された秘密鍵と、それに関連する公開鍵証明書を保管するために一般に利用されるファイルです。今回のファイルには、無線 LAN 用のユーザー証明書、秘密鍵および、CA 証明書が含まれます。
*2 CRT ファイルとは、証明書ファイル形式の一つです。

※BYOD 利用申請後に、『BYOD パスワード通知書』、『無線 LAN 用証明書ファイル』、『プロキシサー ビス用 SSL 証明書(CA 証明書)ファイル』が用意されます。

学校の担当の先生よりメール等で配布された『無線 LAN 用の証明書ファイル』(2.1. BYOD 向け無線 LAN 用証明書のインストール)、『プロキシサービス用 SSL 証明書(CA 証明書)ファイル』(2.2. プロ キシサービス用 SSL 証明書のインストール)はインストールのために BYOD 端末上に移してくださ い。

2.1. BYOD 向け無線 LAN 用証明書のインストール

ここでは、BYOD 向け無線 LAN 用証明書のインストール手順を説明します。

(1) インポートする BYOD 向け無線 LAN 用証明書のファイルをダブルクリックします。
 BYOD 向け無線 LAN 用証明書のファイル名は「<ログイン ID>_1.p12」となります。
 ※この手順書では BYOD 向け無線 LAN 用証明書のファイル名は「nos-test01@edu-g.gsn.ed_1.p12」で記述しております。



(2) 証明書のインポートウィザードが起動します。

"証明書のインポートウィザードの開始"画面が表示されたら、保存場所の「現在のユーザー」を選 択して「次へ」をクリックします。

← ■ 証明者のインボートウィザード	×
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
保存場所 ● 現在のユーザー(C) ○ ローカル コンピューター(L)	
続行するには、[次へ] をクリックしてください。	
	zIL

(3) ファイル名に、インポートするファイルが表示されるので「BYOD 向け無線 LAN 用証明書のファイル名」であることを確認して「次へ」をクリックします。

✤ 毎 証明書のインポートウィザード	×
インボートする証明書ファイル	
インボートするファイルを指定してください。	_
7元4世名(F): Ci¥Users¥alpha¥Desktop¥BYOD¥nos-test01@edu-g.gsn.ed.jp_1.p12 参照(R)	
注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:	
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明會 (.P7B)	
Microsoft シリアル化された証明書ストア (.SST)	
次へ(N) キャンセル	,

(4) 秘密キーのパスワードを入力する画面が表示されるので、『BYOD パスワード通知書』に記載され ている「パスワード」を入力します。入力が完了したら「パスワードの表示」にチェックを入れ て、パスワードが正しく入力されていることを確認し「次へ」をクリックします。

 を閉巻のインボート ウィザード を増生の保護 せキュリティを維持するために、秘密キーはパスワードで保護されています。 や密キーのパスワードを入力してください。 パスワード(P): ・●●●●●●●●●●●● (スワードの表示(D) インボート オブション(1): (スワードの表示(D) インボート オブション(1): (シェイーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 このオーをエクスポート可能にする(M) キーのパッグアップやトランスボートを可能にします。		×
をおまつの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。 必密キーのパスワードを入力してください。 パスワード(P): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	▶ 🥃 証明書のインポート ウィザード	
を書す-の保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。 秘密キーのパスワードを入力してください。 パ(スワード(P): ●●●●●●●●●●●● ② (スワードの表示(D) インボートオブション(D): 「秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 □ このキーをエクスボート可能にする(M) キーのパックアップやトランスボートを可能にします。 □ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスボート不可)(P) ② すべての拡張プロパティを含める(A)		
秘密キーのパスワードを入力してください。 パスワード(P): ●●●●●●●●●●●● ② (スワードの表示(D) インボートオプション(I): □ 秘密キーの保護を強力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。 □ このキーをエクスボート可能にする(M) キーのパックアップやトランスボートを可能にします。 □ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスボート不可)(P) ② すべての拡張プロパティを含める(A)	秘密キーの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。	
秘密キーのパスワードを入力してください。 パスワード(P): ●●●●●●●●●●●●● ② (スワードの表示(D) インボートオブション(I): □ 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 □ このキーをエクスポート可能にする(M) キーのパックアップやトランスポートを可能にします。 □ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P) ② すべての拡張プロパティを含める(A)		
パスワード(P): ●●●●●●●●●●● ② (スワードの表示(D) インボートオブション(I): □ 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 □ このキーをエクスポート可能にする(M) キーのパックアップやトランスポートを可能にします。 □ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P) ② すべての拡張プロパティを含める(A)	秘密キーのパスワードを入力してください。	
 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	バスワード(P):	
 【スワードの表示(D) インボートオブション(I): 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。 このキーをエクスボート可能にする(M) キーのパックアップやトランスボートを可能にします。 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスボート不可)(P) すべての拡張プロパティを含める(A) 	•••••	
インボートオブション(!):	(スワードの表示(D)	
 ○ 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 ○ このキーをエクスポート可能にする(M) キーのパックアップやトランスポートを可能にします。 ○ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P) マ すべての拡張プロパティを含める(A) 	インボート オブション(1):	
 このキーをエクスボート可能にする(M) キーのパックアップやトランスボートを可能にします。 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスボート不可)(P) すべての拡張プロパティを含める(A) 	○ 秘密キーの保護を独力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。	
 ○ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P) ○ すべての拡張プロパティを含める(A) 	□ このキーをエクスポート可能にする(M) キーの / (ックアップやトランフポートを可能に! ます	
▼ すべての拡張プロパティを含める(A)	○ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスボート不可)(P)	
	■ すべての状理プロパティを含める(Δ)	
1		الطرية

(5) 証明書ストア(証明書の保存場所)を指定する画面が表示されたら「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択して「次へ」をクリックします。

	×
★ ● 昼明書のインボートウィザード	
証明書ストア	
証明書ストアは、証明書が保管されるシステム上の領域です。	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
● 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)	
○ 証明書をすべて次のストアに配置する(P)	
証明書ストア:	
参照(R)	
	キャンセル

(6) "証明書のインポートウィザードの完了"画面が表示されたら「完了」をクリックしてウィザードを 終了します。

		×
🔶 🍠 証明書のインボー	トウィザード	
証明書のイン	ソポート ウィザードの完了	
[完了] をクリック	▼ E朝書のインボート ウィザードの完了 CPU1ックすると、証明書がインボートされます。 CPU1ックすると、証明書がインボートされます。 CPU1・ビードで自動的に決定されます CPU1・ビードで自動的に決定されます CPU1・ビード・ビード CPU1・ビード・ビード・ビード CPU1・ビード・ビード CPU1・ビード・ビード・ビード CPU1・ビード・ビード・ビード CPU1・ビード・ビード・ビード CPU1・ビード・ビード・ビード・ビード・ビード・ビード・ビード CPU1・ビード・ビード・ビード・ビード・ビード・ビード・ビード・ビード・ビード・ビード	
次の設定が指定		
内容	PEXPY ワイリードで目前向けに決定されます PFX	
ファイル名	$\label{eq:c:stop} C: \verb"ausers" alpha \verb"ausers" between the stop $	
L		
		1

(7) セキュリティ警告が表示されますので、CA 証明書が「GICT-DC-RADIUS-01」であることを確認し て「はい」をクリックします。

セキュリテ	1 答告 X
4	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:
	GICT-DC-RADIUS-01
	証明書が実際に "GICT-DC-RADIUS-01" からのものであるかどうかを検証 できません。"GICT-DC-RADIUS-01" に連絡して発行者を確認する必要が あります。次の番号はこの過程で役立ちます:
	拇印 (sha1): 3EDC2CAB 0C43C179 B2284386 55A11DC2 019FC2F2
	答告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない拇印付きの証明書をインストール することは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認 識したことになります。
	この証明書をインストールしますか?
	はい(Y) いいえ(N)

(8) BYOD 向け無線 LAN 用証明書のインポートは完了です。「OK」をクリックして閉じてください。



BYOD 向け無線 LAN 用証明書のインストールは以上となります。

2.2. プロキシサービス用 SSL 証明書のインストール

ここでは、プロキシサービスである i-FILTER@Cloud 用の SSL 証明書のインストール手順を説明します。

(1) インポートする i-FILTER@Cloud 用の SSL 証明書のファイルをダブルクリックします。

i-FILTER@Cloud 用の SSL 証明書のファイル名は「sharedpx_ca_sha2.crt」となります。



(2) "証明書"画面が表示されたら「証明書のインストール」をクリックします。

全般 詳細 証	明のバス				
証明書の情報 この CA ルート証明書は信頼されていません。信頼を有効にするにはこの証					
明書を信頼された	-ルート証明機関のストアにインストールしてくだ	さい。			
発行先:	Digital Arts Inc. CA				
発行者:	Digital Arts Inc. CA				
有効期間	2019/10/25 から 2047/03/12				
	証明書のインストール(1) 発行:	者のステートメント(S)			
		ОК			

(3) 証明書のインポートウィザードが起動します。

"証明書のインポートウィザード開始"画面が表示されたら、保存場所の「現在のユーザー」を選択 して「次へ」をクリックします。

← ● 証明者のインボートウィザード	×
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機關によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
保存場所 ● 現在のユーザー(C) ○ ローカル コンピューター(L)	
続行するには、[次へ] をクリックしてください。	
次へ(N) キャンセル	

(4) 証明書ストア(証明書の保存場所)を指定する画面が表示されたら「証明書をすべて次のストアに 配置する」を選択して「参照」をクリックします。

◆ ■ 証明書のインボートウィザード	×
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
 ○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U) ● 証明書をすべて次のストアに配置する(P) 証明書ストア: 参照(R) 	
次へ(N) キャンt	.11

(5) "証明書ストアの選択"画面が表示されるので「信頼されたルート証明機関」を選択して「OK」をクリックします。

証明書ストアの選択	×
使用する証明書ストアを選択してください(C)	
	_
- <u> </u> 個人 - <mark> </mark> 信頼されたルート証明機関	
	1
□ 物理ストアを表示する(S)	
OK キャンセル	

(6) 証明書ストアに「信頼されたルート証明機関」が選択されたことを確認して「次へ」をクリックします。

🚰 証明書の1	ンポートウィザード					
証明書ストア						
証明書	ストアは、証明書	が保管されるシス	テム上の領域で	す。		
Windo	ws に証明書ストフ	を自動的に選択	させるか、証明	書の場所を指	定することが	できます。
0	証明書の種類に書	きづいて、自動的(こ証明書ストア	を選択する(U)		
0	証明書をすべて次	のストアに配置す	3(P)			
	証明書ストア:					
	信頼されたルート	証明機関				参照(R)
-						

(7) "証明書のインポートウィザードの完了"画面が表示されたら「完了」をクリックしてウィザードを 終了します。

	×
🔶 📴 証明書のインボート ウイザード	
証明書のインポート ウィザードの完了	
[完了]をクリックすると、証明書がインポートされます。	
次の設定が指定されました。	
 ユーザーが違択した証明書ストア 信頼されたルート証明機関 内容 証明書 	
	_
完了(F)	キャンセル

(8) セキュリティ警告が表示されますので、CA 証明書が「Digital Arts Inc.CA」であることを確認して 「はい」をクリックします。

セキュリテ	1 警告	×
4	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています: Digital Arts Inc. CA 証明書が実際に "Digital Arts Inc. CA" からのものであるかどうかを検証で きません。"Digital Arts Inc. CA" に連絡して発行者を確認する必要があり ます。次の番号はこの過程で役立ちます: 拇印 (sha1): CB49A7A8 4380A1AB E1C65B9E 883CD972 89AB5A83 答告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない拇印付きの証明書をインストール	5
	することは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認 識したことになります。 この証明書をインストールしますか?	
	(はい(Y) いいえ(N)	ן כ

(9) i-FILTER@Cloud 用の SSL 証明書のインポートは完了です。「OK」をクリックしてください。



(10) "証明書"画面の「OK」をクリックして閉じてください。

50	証明書	×
£	般 詳細 証明のバス	
	証明書の情報 この CA ルート証明書は信頼されていません。信頼を有効にするにはこの証明書を信頼されたルート証明機関のストアにインストールしてください。	-
	発行先: Digital Arts Inc. CA	
	発行者: Digital Arts Inc. CA	
	有効期間 2019/10/25 から 2047/03/12	
	証明書のインストール(I) 発行者のステートメント(S)	
	ОК	

プロキシサービス用 SSL 証明書のインストールは以上となります。

2.3. BYOD 向け無線 LAN 接続実施

ここでは学校で BYOD 向け無線 LAN へ接続する手順を説明します。

(1) デスクトップ画面下にあるタスクバーの「ネットワーク」アイコン(地球儀)をクリックします。

へ あ ⊕ ∿ ■	16:49 2022/01/20 2
-----------	-----------------------

(2) Wi-Fi をオンにします。

ネットワーク画面の Wi-Fi アイコン(扇状)の右側にある「>」をクリックします。



(3) 右上のバーが無効(グレー)になっている場合は、バーを選択して Wi-Fi を有効(ブルー)にしま す。

← Wi-Fi	
Wi-Fi がオフです	
Wi-Fi をオンにして、利用可能な Wi-Fi ネットワ ます。	ークに接続し
Wi-Fi をもう一度オンにする	
手動	~
その他の Wi-Fi 設定	

(4) Wi-Fi 一覧が表示されたら、BYOD 向けの SSID (GunmaSchool_BYOD) をクリックします。

← Wi-Fi	
GunmaSchool_BYOD	
A	
A	
() () ()	
その他の Wi-Fi 設定	

(5) ログイン画面が表示されたら「証明書を使って接続する」をクリックします。

÷	Wi-Fi
	GunmaSchool_BYOD 接続中
	ユーザー名とパスワードを入力してください
	ユーザー名
	パスワード
	証明書を使って接続する
	ОК ++>>セル

(6) 接続の画面が表示されたら「接続」をクリックします。

~	Wi-Fi	
A	GunmaSchool_BYOD 接続中	
	接続を続けますか? この場所に GunmaSchoo 予想される場合は、そのま でない場合は、名前が同じ ある可能性があります。 証明書の詳しい内容の表	ol_BYOD が存在すると ま接続してください。そう じでも別のネットワークで 示
	接続	キャンセル

(7)「接続済み、セキュリティ保護あり」画面が表示されていれば、無線 LAN へ接続は完了です。

← Wi-Fi	
GunmaSchool_BYOD 接続済み、セキュリティ係	「
	切断

Windows 11 における BYOD 向け無線 LAN 接続は以上となります。

2.4. プロキシ設定確認

ここでは Windows 11 のプロキシ設定の確認手順を説明します。

BYOD を学校で利用する場合はプロキシの自動検出機能を有効にしておく必要があります。Windows 11 ではデフォルトで自動検出機能がオンですが、念のため下記の画面で確認します。

(1) デスクトップ画面下にあるタスクバーの「スタート」ボタンをクリックして「設定」ボタン(歯車 マーク)をクリックします。



(2) "設定"画面が表示されたら「ネットワークとインターネット」をクリックします。



(3) "ネットワークとインターネット"画面が表示されたら、右下にある「プロキシ」をクリックします。



(4) "プロキシ"画面の「設定を自動的に検出する」が「オン」になっていることを確認したら、ウイン ドウを閉じます。もし、「オン」でなければ「オン」にしてください。



プロキシ設定確認は以上となります。

2.5. Web アクセス実施、プロキシサービスヘログイン

ここでは Web にアクセスする手順を説明します。Microsoft Edge ブラウザを立ち上げて Web アクセ スを実施するとプロキシサービス利用の認証画面が表示されますので、ID とパスワードを入力してく ださい。認証が成功すると Web ページが表示されます。

(1) デスクトップ画面下にあるタスクバーの「Microsoft Edge」ボタンをクリックします。



(2) ブラウザからホームページアクセス時に下図の認証画面が表示されます。「ユーザー名」にはパス ワード通知書にある「i-FILTER アカウント名」を、「パスワード」にはパスワード通知書の「パス ワード」をそれぞれ入力して「ログイン」をクリックします。

by https://ict-support.gsn.ed.jp x +			-	ø	×
←	ŝ	£≡	Ē	۲	
このサイトにアクセスするにはサインインしてください プロキシ http://dastc-1954.px.digitalartscloud.com.443 には、ユーザー名とパスワード が必要です。 このサイトへの薄掃信は安全ではありません					
1-7-6					
サインイン キャンセル					
🖬 🖉 🖬 🖬 🖉 📾	× A•	ক ব×	₽ ₂₀	17:0 22/01/2	9 1

(3) ログインに成功すると、プロキシサービス経由で Web アクセスが可能となり、アクセス許可のサ イトの場合は下図のように Web ページが表示されます。

※下図はアクセス許可のサイトが表示された場合の例となります。

□ ホーム・群馬県ICT活用教育サポート × +				=	Ø	×
\leftrightarrow \rightarrow O $rightarrow$ https://ict-support.gs	red.jp	A [%] t ∂	£]≡	œ	(2)	
群馬県ICT活用教育サポー	サイト		ログ・	イン		
• ** • ホーム	群馬県ICT活用教育サポートサイトへようこそ!!			_		
FAQ(頻繁な質問)	このサイトは、1人1台端末の有効な活用に向けて、教職員の皆さん(コンテンツによっては児童生徒も活用。 サイトです。	J能!!)をサオ	R- 197	5		
活用のイメージ作り	各種マニュアルや端末のトラブル対応等の情報を掲載していきます。					
活用事例(授業、校務等)						
Googleサービスの活用						
スタディサプリの活用		1				

※下図はアクセス不許可のサイトを開いた場合の例となります。

Duyyahala. × +						
	A	ŝõ	£≡	Ð	۲	
i-FILTER.						
このページは「i-FILTER@Cloud」によりブロックされました。						
URL http://kendama.net/						
ブロック理由 共通リスト:ブラックリスト(カテゴリ1)						
IPアドレス 210.149.228.198						
認証ユーザー名 nos-test01@edu-g.gsn.ed.jp						
i-FILTER ∕ @ 1999 Digital Arts Inc.						_
DateTime: 2022/02/08 10:41:33						

※備考

Windows 11 でアプリケーションを起動した際に、下図のようにサーバー「daatc-1954.px.digitalartscloud.com」がユーザー名とパスワードを要求する Windows セキュリティ画面 が表示される場合もあります。これはアプリケーションが起動の際に Web アクセスを行い、プロ キシサーバーの利用が必要になったためです。その場合は、「ユーザー名」にはパスワード通知書 にある「i-FILTER アカウント名」を、「パスワード」にはパスワード通知書の「パスワード」をそ れぞれ入力して「OK」をクリックして認証してください。

Windows セキュリティ	×
設定	
サーバー daatc-1954.px.digitalartsclo 要求しています。	bud.com がユーザー名とパスワードを
サーバーからの報告: "i-FILTER@Cloud	"。
ユーザー名	
パスワード	
✓ 資格情報を記憶する	
ОК	キャンセル

Windows 11 における BYOD 端末の Web アクセス手順は以上となります。

3. 証明書削除手順

県立学校を卒業及び転校等で群馬県立学校から離れる場合、BYOD にインストールした証明書を削除 する場合の手順を説明します。削除手順のイメージは下図の通りとなります。

注意:以降の作業を実施すると校内無線 LAN 環境に接続できなくなります。

- (1) プロキシサービス用SSL証明書の削除
- (2) BYOD向け無線LAN用証明書の削除



3.1. プロキシサービス用 SSL 証明書の削除

ここでは、プロキシサービスである i-FILTER@Cloud 用の SSL 証明書の削除手順を説明します。

(1)「スタート」ボタンを右クリックして「ファイル名を指定して実行」をクリックします。

	アプリと機能
	モビリティ センター
スタートボタン	電源オプション
	イベント ビューアー
	システム
	デバイス マネージャー
	ネットワーク接続
	ディスクの管理
	コンピューターの管理
	Windows ターミナル
	Windows ターミナル (管理者)
	タスク マネージャー
	設定
	エクスプローラー
	検索
	ファイル名を指定して実行
	シャットダウンまたはサインアウト >
	デスクトップ

(2) "ファイル名を指定して実行"画面が表示されたら、名前に「mmc」と入力して「OK」をクリックします。

ファイル名を指定して実行 >	<
実行するプログラム名、または開くフォルダーやドキュメント名、インター ネットリソース名を入力してください。	
名前(O): mmc ~	
🐓 このタスクは管理者特権で作成されます。	
OK キャンセル 参照(B)	

(3) "コンソール"画面が表示されたら「ファイル」タブから「スナップインの追加と削除」を選択しま す。



(4) "スナップインの追加と削除"画面が表示されたら、利用できるスナップインから「証明書」を選択 して「追加」をクリックします。

7+******	N115-	אן אן-עער 🥅	
	Nine (Com		14.150/清末(八)
■ セキュリティ テノノレート	Microsoft Corp		削除(R)
マレイエッティが短しされた…	Microsoft Corp		
タスクスケジューラ	Microsoft Corp		した主な手上のの
ディスクの管理	Microsoft and V.		上八移動(0)
デバイスマネージャー	Microsoft Corp		下へ移動(D)
のパフォーマンスモニター	Microsoft Corp	追加(A) >	
コフォルダー	Microsoft Corp		
ポリシーの結果セット	Microsoft Corp		
💂 ローカル ユーザーとグループ	Microsoft Corp		
日間の管理	Microsoft Corp		
共有フォルダー	Microsoft Corp		
承認マネージャー	Microsoft Corp		
	Microsoft Corp.		詳細設定(V)

(5) "証明書スナップイン"画面が表示されたら、このスナップインで管理する証明書の「ユーザーアカ ウント」を選択して「完了」をクリックします。

証明書スナップイン		×
このスナップインで管理する証明書: ユーザーアカウント(M) サービス アカウント(S) コンピューター アカウント(C) 		
	< 戻る(B) 完了 キャンセル	

(6) "スナップインの追加と削除"画面の、選択されたスナップインに「証明書-現在のユーザー」が格納 されていることを確認したら「OK」をクリックします。

はナップイン	ベンダー	温いられたスケックトライと).	拡張の編集(X)
カキュリティテンプレート	Microsoft Corp	□□ 証明書 - 現在のユーザー	
* ビデュリティ ブノフレート	Microsoft Com		削除(R)
セキュリティの構成と公析	Microsoft Corp		
タスク スケジューラ	Microsoft Corp		レムギクテトパリ
ディスクの管理	Microsoft and V.		上へ後期(0)
デバイスマネージャー	Microsoft Corp		下へ移動(D)
)パフォーマンス モニター	Microsoft Corp	追加(A) >	
フォルダー	Microsoft Corp		
ポリシーの結果セット	Microsoft Corp		
	Microsoft Corp		
の印刷の管理	Microsoft Corp		
共有フォルダー	Microsoft Corp		
承認マネージャー	Microsoft Corp		
■証明書	Microsoft Corp		詳細設定(V)

- (7) "コンソール"画面のコンソールルートにある「証明書-現在のユーザー」の左側にある「>」をク
 - リックします。

א-א א-עיבן - רא-עיבן	-	o x
National Sector (A) 表示(V) お気に入り(O) ウィンドウ(W) ヘルブ(H)		- 8 ×
Ci コンソール ルート 名前	操作	
> 🖓 証明書 - 現在のユーザー 🖓 証明書 - 現在のユーザー	コンソール ルート	
	他の操作	•

(8)「信頼されたルート証明機関」の中の「証明書」をクリックします。

発行先および発行者が「**Digital Arts Inc. CA**」となっている証明書が i-FILTER 用の SSL 証明書で す。

※それ以外の証明書の削除はしないでください!



(9) i-FILTER 用の SSL 証明書にカーソルをあわせ、右クリックして「削除」を選択します。



(10) 証明書の削除を続行する場合は「はい」をクリックします。



(11) 証明書の削除を続行する場合は「はい」をクリックします。



(12) i-FILTER 用の SSL 証明書が削除されていることを確認してください。



プロキシサービス用 SSL 証明書の削除は以上となります。

引き続き【3.2. BYOD 向け無線 LAN 用証明書の削除】を実施してください。

3.2. BYOD 向け無線 LAN 用証明書の削除

ここでは、BYOD 向け無線 LAN 用証明書の削除手順を説明します。

(1) 最初に無線 LAN 用ユーザー証明書を削除します。

"コンソール"画面の「個人」の中の「証明書」をクリックします。

発行先が<ロ**グイン ID**>、発行者が「GICT-DC-RADIUS-01」となっている証明書が無線 LAN 用 ユーザー証明書となります。

※この手順書では BYOD 向け無線 LAN 用証明書のファイル名は「nos-test01@edu-g.gsn.ed.jp」で記述します。 **それ以外の証明書の削除はしないでください**!

🖀 certmgr - [証明書 - 現在のユーザー	¥個人¥証明書]		() <u></u> ()	D	×
ファイル(F) 操作(A) 表示(V) ヘル	レプ(H)				
🗢 🄿 🖄 📰 🔏 🖬 🗙 🗉	1 🔒 🛛 🖬				
🗊 証明書 - 現在のユーザー	発行先 ^	発行者			有
 	nos-test01@edu-g.gsn.ed.jp	GICT-DC-RADI	US-01		20
		-			
個人 ストアには1個の証明書があります。					

(2) BYOD 向け無線 LAN 用証明書にカーソルをあわせ、右クリックして「削除」を選択します。

Reference of the second of the se		o ×	
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🚈 🔏 🛍 🖌 🖾 🖬			
□ 証明書 - 現在のユーザー ◇	発行者 -g.gsp.ed.inGICT-DC-RADIUS-01	有 20	
 ○○ 信頼されたルート証明機関 >○○ 信頼されたの信頼 	開く(O) 	十 月11-11-15-14	
 > 中間証明機関 > Active Directory ユーザーオブジ > 信頼された発行元 > 信頼されたいない証明書 > サードパーティルート証明機関 > 信頼されたユーザー > 信頼されたユーザー > クライアント認証発行者 	切り取り(T) コピー(C) <u>利除(D)</u> プロパティ(R) ヘルプ(H)	49999 CH	床で送扒
 > □ Local NonRemovable Certific: > □ 証明書の登録要求 > □ スマートカードの信頼されたルート 			
選択範囲を削除します。			

(3) 証明書の削除を続行します場合は「はい」をクリックします。



(4) BYOD 向け無線 LAN 用証明書が削除されていることを確認します。

🦀 certmgr - [証明書 - 現在のユーザー	¥個人¥証明	書]			×	
ファイル(F) 操作(A) 表示(V) ヘル	/プ(H)					
🗢 🔿 🙍 💼 🗟 🖬						
□ 証明書 - 現在のユーザー	発行先	^ 発行者			有	
✓ ■ 個人 ○ 証明書		このビューに表示する項目はお	ありません。			
> 🧰 信頼されたルート証明機関						
> 🧾 エンダーフライ Xの1言類 > 🎬 中間証明機関						
> 📔 Active Directory ユーザー オブジ						
> 🧾 信頼された発行元 > 🎬 信頼されていない証明書		BYOD 向け無線 LAN 用証	:明書か削防	きれて	いること	を催認
> ジ サードパーティルート証明機関						
> 🧾 信頼されたユーザー						
> 📫 クライアント認証発行者						
> Local NonRemovable Certifici						
> 🚞 証明書の登録要求						
> 📔 スマートカードの信頼されたルート						

(5) 次に CA 証明書を削除します。「信頼されたルート証明機関」の中の「証明書」をクリックします。 発行先および発行者が「GICT-DC-RADIUS-01」となっている証明書が CA 証明書です。 ※それ以外の証明書の削除はしないでください!

\overline 🖀 certmgr - [証明書 - 現在のユーザー	¥信頼されたルート証明機関¥証明書]	– o ×
ファイル(F) 操作(A) 表示(V) ヘル	ノプ(H)	
🗢 🔿 🖄 📷 🖌 🖬 🗙 🖬	1 🗟 👔 🖬	
 □ 証明書 - 現在のユーザー ○ 個人 ○ 信頼されたルート証明機関 ○ エンターブライズの信頼 ○ 中間証明機関 ○ Active Directory ユーザーオブジ ○ 信頼された発行元 ○ 信頼された発行元 ○ 信頼されたれート証明機関 ○ ヴードパーティルート証明機関 ○ 信頼されたユーザー ○ クライアント認証発行者 ○ Local NonRemovable Certifica ○ 証明書の登録要求 > ○ スマートカードの信頼されたルート 	発行先 DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance EV Ro Equifax Secure Certificate Auth GICT-DC-RADIUS-01 GlobalSign GlobalSign Root CA Microsoft Authenticode(tm) Ro Microsoft ECC Product Root Cer Microsoft ECC Product Root Cer Microsoft Root Authority Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth	発行者 DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance EV Root Equifax Secure Certificate Authority GICT-DC-RADIUS-01 GlobalSign GlobalSign Root CA Microsoft Authenticode(tm) Root Microsoft ECC Product Root Certifi Microsoft ECC Product Root Certificate Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authori Microsoft Root Certificate Authori
信頼されたルート証明機関ストアには31個	回の証明書があります	

(6) CA 証明書にカーソルをあわせ、右クリックして「削除」を選択します。



(7) 証明書の削除を続行します場合は「はい」をクリックします。



(8) ルートストアからの削除は「はい」をクリックします。

ルート証明]書ストア	\times
1	次の証明書をルートストアから削除しますか? サブジェクト: GICT-DC-RADIUS-01, Gunma-ken, JP 発行者: 自己発行 有効期間: 2020年11月20日から2030年11月19日まで ジリアル者号: 00CCE1D1 676DD9C8 55 揖印 (sha1): 3EDC2CAB 0C43C179 B2284386 55A11DC2 019FC2F2 揖印 (md5): 1DD68681 C560412C 6B97397B D50BA3B5	
	はい(Y) いいえ(N)	

(9) CA 証明書が削除されていることを確認します。



(10) 証明書の削除は完了です。画面右上の「×」ボタンをクリックし、コンソールの設定は保存しな いため「いいえ」をクリックしてコンソール画面を閉じてください。



BYOD 向け無線 LAN 証明書の削除は以上となります。

以上