NEC
NECソリューションイノベータ

InfoCage FileShell プロテクタ
for NIAS
利用ガイド

InfoCage

InfoCage FileShell プロテクタ for NIAS
Version 6.3
利用ガイド
（0630N02）

はじめに

このたびは、NEC ソリューションイノベータ株式会社の InfoCage FileShell 製品 をお買い求めいただき誠にありがとうございます。

InfoCage FileShell は、電子ファイル自身にセキュリティ情報を持たせた暗号化をおこなうことで、

利用者の操作性を損なうことなく重要な情報を永続的に保護する機密情報保護ソフトウェアです。

ご使用になる前に本書をよくお読みになり、製品の取り扱いを十分にご理解ください。

■ 商標について

- Microsoft および Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- InfoCage は NEC ソリューションイノベータ株式会社の登録商標です。
- NIAS は、日本電気株式会社の登録商標です。
- その他、本書に記載されている会社名、商品名は各社の登録商標または商標です。

■ 免責事項

本書および本システムは、ライセンス契約に基づいて使用することができます。
ライセンス契約で明示的に定められていないかぎり、NEC ソリューションイノベータ株式会社は製品、およびその関連文書について、明示的にも暗黙的にも、商品性に関する保証、特定目的への適合性に関する保証、取り扱い、使用、または取引行為に伴う保証について一切の責任を負いません。

本書中のサンプル画面で使用している名称は、すべて架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

本書について

本書は本製品を正しく運用し、効果的に活用するための手引きです。運用を開始する前や運用中に、機能・操作を確認するためにご利用ください。

本書は、InfoCage FileShell プロテクタ for NIAS の利用者を対象としています。

また、本書は操作手順や画面の表示を主に Windows Server 2016 の場合を例に記載しています。
適宜、お使いのオペレーティングシステムに読みかえてください。

ご注意：本書の一部、または全部を流用・複写することはできません。

本書中の記号について

本書中では、以下の記号を使用しています。これらの記号の意味を正しくご理解になり、本書をお読みください。

記　号	説　　明
Notice	システムの取り扱いで守らなければならない事柄や特に注意すべき点、確認すべき点を説明します。
参照	関連する内容が記載されているページを紹介しています。
Operation	操作手順を示します。

参考資料について

本書中では、参考資料として以下のガイドを参照するように説明しています。

項　目	ガ　イ　ド　名	番 号
インストールガイド	InfoCage FileShell インストールガイド	0630Snn
管理者ガイド	InfoCage FileShell 管理者ガイド	0630Knn
NEC File Protection Edition 管理者ガイド	InfoCage FileShell NEC File Protection Edition 管理者ガイド	0630RKnn
NEC File Protection Edition 利用ガイド	InfoCage FileShell NEC File Protection Edition 利用ガイド	0630RUnn

＊ 末尾の「nn」には、「01」、「02」などの数字(版数)が入ります。
版数は、プログラムやマニュアルに変更があった場合に更新されます。

用語の定義

本書では、システム操作の説明に以下のような用語を用いています。本書を確認するにあたって前提としてご理解ください。

用　語	説　　明
NIAS (NEC Information Assessment System)	NEC が提供するファイルサーバー統合管理ソフトウェアのことです。 ファイルサーバーの整理、アクセス権管理、リソース管理、個人情報検出などの機能があります。
FileShell SDK	本ソフトウェアの動作に必要となるソフトウェアのことです。FileShell SDK はファイルの保護、および保護解除をするためのインタフェースを提供します。
オンプレミス RMS	RMS サーバーを自社に構築する運用方法です。Microsoft 社の Active Directory Rights Management Services を利用します。
Azure RMS	RMS サーバーを自社に構築せず、クラウドサービスを利用する運用方法です。Microsoft 社の Azure Rights Management を利用します。
MIP	Microsoft Information Protection の略称で、Microsoft 社が提供する情報保護ソリューションのことです。本書では MIP と記載します。 Microsoft Information Protection の詳細については、Microsoft 社の Web サイト等をご参照ください。
ラベル	MIP にて、文書に付与される情報です。 ファイルの保護(暗号化)がおこなえるラベルには権利ポリシーが含まれています。ファイルの分類／保護に使用します。
分類	ファイルにラベルを付与することです。
NEC File Protection Edition(NFP)	オンプレミスまたはクラウドの RMS 基盤を使用せず、NEC 独自の方式により「ファイルの保護」や「利用の制限(権限による制御)」などをおこなう仕組みのことです。 「NFP 権利ポリシー認証機能」が利用できるサーバー認証版と、サーバーレスでも利用可能な鍵配布版の 2 種類があります。
NFP 権利ポリシー ／ NFP 権利ポリシーテンプレート	NFP で、ファイルを保護/保護解除するために使用する「共通鍵」やファイル利用時の「権限」および有効期限の設定が埋め込まれた情報のことです。
OfficeIRM 形式	Office アプリケーションでサポートしている保護形式です。
Microsoft 互換形式	Microsoft Office ファイル、および PDF ファイルをラベルを用いて出力した際の形式です。Microsoft 互換形式で出力したファイルには、ラベルが付与されます。 また、ファイルの保護(暗号化)がおこなえるラベルを用いて出力したファイルは、ラベルの付与と同時に保護されます。
FileShell 形式	FileShell 独自の保護形式です。 なお、本書では、RMS の権利ポリシーテンプレートを用いて出力(保護)する形式を「FileShell 形式」、MIP のラベルを用いて主力(保護/分類)する形式を「FileShell(ラベル)形式」と記載しています。
NFP 形式	RMS を使用しない NEC 独自の保護形式です。

目 次

第 1 章　FileShell プロテクタ for NIAS について 1

1.1　特長 1

1.2　機能 1

1.3　動作環境について 1

1.4　FileShell プロテクタ for NIAS の運用までの流れ 3

第 2 章　注意事項 4

2.1　運用上の注意事項 4

2.1.1　共通の注意事項 4

2.1.2　OfficeIRM/FileShell 形式の保護使用時の注意事項 5

2.1.3　Microsoft 互換/FileShell(ラベル)形式の分類/保護使用時の注意事項 7

2.1.4　NFP 形式の保護使用時の注意事項 7

第 3 章　FileShell プロテクタ for NIAS のインストール 8

3.1　運用環境構築の流れ 8

3.2　必要なソフトウェアのインストール 8

3.3　オンプレミスの RMS サーバーへの接続に必要な設定 9

3.3.1　RMS 証明パイプラインに権限を追加する 9

3.4　MIP/Azure RMS を利用する場合に必要な情報の設定と取得 10

3.4.1　Azure Portal でのアプリケーションの登録 10

3.4.2　API アクセス許可の追加 12

3.4.3　クライアントシークレットの作成 15

3.4.4　Azure RMS のライセンスサーバー、および認証サーバーURL の取得 16

3.5　権利ポリシーテンプレートの準備 18

3.5.1　オンプレミス RMS サーバー上の権利ポリシーテンプレートの取得と保存 18

3.5.2　Azure RMS サーバー上の権利ポリシーテンプレートの取得と保存 19

3.5.3　NFP 権利ポリシーテンプレートの取得と保存 21

3.6　FileShell プロテクタ for NIAS のインストール 23

3.6.1　インストールパッケージの展開 23

3.6.2　NFP の緊急保護解除用の公開鍵の取得 24

3.6.3　インストーラーの設定 26

3.6.4　NFP の緊急保護解除に関する設定例 31

3.6.5　インストール 33

3.6.6　バージョンアップインストール 36

3.7　RMS サーバーの接続設定 36

3.8　権利ポリシーテンプレートのインポート 37

3.8.1　Office IRM/FileShell 形式で保護する場合 37

3.8.2 NFP 形式で保護する場合 39
3.9 ラベル ID の取得 41

第 4 章 環境設定ツール 43
4.1 機能一覧 43
4.2 起動方法 43
4.3 環境設定ツールの操作 43
4.3.1 RMS 認証情報設定 43
4.3.2 権利ポリシーテンプレートの管理 46
4.3.3 ログ出力情報設定 49
4.3.4 オプション設定 50
4.3.5 動作環境表示 51
4.3.6 設定情報ファイル出力 52

第 5 章 NIAS のインストール 53
5.1 NIAS 製品本体、エージェントのインストール 53
5.2 保護(暗号化)メニューの画面表示設定 53
5.2.1 プロパティファイル（日・英）を修正する 53
5.3 FileShell プロテクタ for NIAS の呼び出し設定 55
5.4 保護(暗号化)の実行方法 58
5.4.1 検索画面から保護(暗号化)する 58
5.4.2 個人情報画面から保護(暗号化)する 59

第 6 章 アンインストール 60

第1章 FileShell プロテクタ for NIAS について

1.1 特長

FileShell プロテクタ for NIAS は、NIAS と連携する InfoCage FileShell のオプション製品です。
NIAS 環境にインストールすることで、NIAS が検出したファイルを Office IRM/FileShell 形式、Microsoft 互換/FileShell1(ラベル)形式、または NFP 形式で保護(暗号化)することが可能になります。

1.2 機能

FileShell プロテクタ for NIAS には、次の機能があります。

● **NIAS によるファイル保護機能**

NIAS が検出したファイルを、InfoCage FileShell の Office IRM/FileShell 形式、Microsoft 互換/FileShell(ラベル)形式または NFP 形式で保護(暗号化)します。
保護されたファイルは、InfoCage FileShell がインストールされたクライアント PC で、FileShell の管理者が設定したポリシー(ユーザー/グループごとの権限設定)に基づき、ファイルの閲覧、編集、印刷などをおこなうことができます。

1.3 動作環境について

動作環境は以下のとおりです。

■ FileShell プロテクタ for NIAS

Windows Server

		Windows Server		
		2022	2019	2016
ハードウェア	CPU	2.0GHz 相当以上の x86 互換アーキテクチャのプロセッサ		
	メモリ	2GB 以上		
	ハードディスク	本ソフトウェアのインストールに 40MB 以上の空き容量が必要 (*2)		
	ネットワークインタフェース	100Mbps 以上(IPv4 のみ)		
OS (*1)	エディション	Standard	Standard	Standard
	更新プログラム	なし	なし	なし
	言語	日本語/英語		
必須ソフトウェア	InfoCage FileShell SDK (*3)	○	○	○
	Microsoft .NET Framework 4.7.2 以上 (*4) (*5)	○	○	○
	AIPService PowerShell モジュール (*6)	○	○	○
	RMS Client 2.1 (*7) (*8)	○	○	○
	Visual Studio 2015、2017、2019、および 2022 用 Visual C++再頒布可能パッケージ (*8)	○	○	○

Windows Storage Server

		Windows Storage Server 2016
ハードウェア	CPU	2.0GHz 相当以上の x86 互換アーキテクチャのプロセッサ
	メモリ	2GB 以上
	ハードディスク	本ソフトウェアのインストールに 40MB 以上の空き容量が必要 (*2)
	ネットワークインタフェース	100Mbps 以上(IPv4 のみ)
OS (*1)	エディション	Standard
	更新プログラム	なし
	言語	日本語/英語
必須ソフトウェア	InfoCage FileShell SDK (*3)	○
	Microsoft .NET Framework 4.7.2 以上 (*4) (*5)	○
	AIPService PowerShell モジュール (*6)	○
	RMS Client 2.1 (*7) (*8)	○
	Visual Studio 2015、2017、2019、および 2022 用 Visual C++再頒布可能パッケージ (*8)	○

(*1) Microsoft 社から提供される最新セキュリティパッチを適用してください。

(*2) 分類／保護の際には、処理対象ファイルが存在するドライブに、 ”[処理対象ファイルサイズ] × 3 バイト以上“ が必要です。

(*3) 本ソフトウェアのインストール時に同時にインストールされます。動作に必要となるため、アンインストールしないでください。

(*4) Windows Server 2016、および Windows Storage Server 2016 をご利用の場合は、後述(*8)の「Microsoft ダウンロードセンター」よりダウンロードする必要があります。それ以外の対応 OS では OS のデフォルトでインストールされています。動作に必要となるため、削除しないでください。

(*5) OS と同じ言語の.NET Framework Language Pack も必要です。

(*6) FileShell で MIP を利用する場合に必要です。Windows PowerShell を利用してインストールする必要があります。

参照 インストール方法については、「3.4.4 Azure RMS のライセンスサーバー、および認証サーバー URL の取得」を参照してください。

(*7) ファイルの保護にオンプレミスの AD RMS を利用する場合に必要です。

(*8) 「Microsoft ダウンロードセンター」よりダウンロードする必要があります。
以下の Web サイトよりファイルをダウンロードしてから、インストールしてください。

(2023/12/15 時点)

タイトル、URL	備考
Microsoft .NET Framework 4.7.2 https://dotnet.microsoft.com/ja-jp/download/dotnet-framework/net472	各言語用の Language Pack も本ページ内のリンクからダウンロードできます。
Visual Studio 2015、2017、2019、および 2022 用 Visual C++再頒布可能パッケージ https://docs.microsoft.com/ja-JP/cpp/windows/latest-supported-vc-redist?view=msvc-170	64bit(x64)用モジュールを適用してください。
RMS Client 2.1 https://www.microsoft.com/ja-jp/download/details.aspx?id=38396	-

1.4 FileShell プロテクタ for NIAS の運用までの流れ

FileShell プロテクタ for NIAS の運用までの流れは、以下のとおりです。

No.	項目	内容	参照
1	必要なソフトウェアのインストール	FileShell プロテクタ for NIAS が動作するために必要なソフトウェアをインストールします。	3.2
2	RMS サーバー接続に必要な設定および情報の取得	FileShell プロテクタ for NIAS を使用するサーバーマシンが RMS サーバーに接続するために必要な設定および情報の取得をおこないます。 ＊ NFP 形式での保護のみを使用する場合は必要ありません。	3.3
3	権利ポリシーテンプレートの準備	保護時に利用する権利ポリシーテンプレートを準備します。	3.5
4	FileShell プロテクタ for NIAS のインストール	サーバーマシンに本ソフトウェアをインストールします。	3.6
5	権利ポリシーテンプレートのインポート	保護時に利用する権利ポリシーテンプレートをサーバーマシンにインポートします。	3.8
6	初期設定	InfoCage FileShell SDK 環境設定ツール(以降、「環境設定ツール」と記載します)を使用して、RMS サーバー、Azure RMS または NFP 権利ポリシーの設定をします。	第 4 章
7	NIAS 製品本体、エージェントのインストール	NIAS 製品本体、もしくはエージェントをインストールします。	5.1
8	NIAS 整理メニューの追加および実行	NIAS の「検索」画面や「個人情報」画面に、FileShell プロテクタ for NIAS を使用して保護(暗号化)をおこなう整理メニューを追加し、実行します。	5.2 5.3 5.4

＊ 本ソフトウェアおよび NIAS のインストール順は、上記と逆(NIAS 製品本体、本ソフトウェアの順)でも問題ありません。
この場合、下記の順で読み進めてください。

- 「5.1 NIAS 製品本体、エージェントのインストール」
- 上記表の No.1～6
- 「5.2 保護(暗号化)メニューの画面表示設定」以降

＊ 既に NIAS 製品本体の環境が構築済みの場合は、下記の順で読み進めてください。
なお、この場合、NIAS 製品本体が Ver.4.1 以降である必要があります。
上記 Ver.以下の場合は、アップデートをおこなってください。

- 上記表の No.1～6
- 「5.2 保護(暗号化)メニューの画面表示設定」以降

＊ NIAS エージェントのみインストールしたサーバーについても FileShell プロテクタ for NIAS のセットアップは必要になりますのでご注意ください。

第2章 注意事項

2.1 運用上の注意事項

2.1.1 共通の注意事項

＊ 本ソフトウェアのインストーラーは、必ずインストーラ作成支援ツールを使用して作成してください。テキストエディタ等によるインストーラー設定ファイルの編集はおこなえません。

＊ 本ソフトウェアをインストールすると、InfoCage FileShell SDK も同時にインストールされます。
動作に必要となるため、InfoCage FileShell SDK はアンインストールしないでください。

＊ 本ソフトウェアでは、FileShell Ver5.0 以下のインストーラ作成支援ツールで作成された本ソフトウェアのインストーラー、およびインストール設定ファイル(setup.ini)は使用できません。インストールをおこなう際は、「3.6 FileShell プロテクタ for NIAS のインストール」の手順にしたがって、ご利用の環境に応じたインストーラーを作成し、実施してください。

＊ 本ソフトウェアは、InfoCage FileShell SDK を除く、InfoCage FileShell の他のソフトウェアと共存させることはできません。

＊ 本ソフトウェアの動作には、本ソフトウェアがインストールされたサーバーマシンが所属するドメインの以下のいずれかのユーザー(タイプ)のアカウントで実行する必要があります。
- administrator (ユーザー)
- administrators グループに所属するユーザー
- Backup Operators グループに所属するユーザー

＊ 本ソフトウェアで分類(ラベルの付与)、保護(暗号化)およびそれらの適用を解除するファイルに対して、前述したアカウントが以下のアクセス権限を有している必要があります。
- 読み取り
- 書き込み
- 読み取りと実行
- 変更
- フォルダーの内容の一覧表示
- 所有権の取得
- アクセス許可の読み取り
- アクセス許可の変更

＊ 保護および保護解除後のファイルは、ファイルシステム上ではファイルが存在しているフォルダーと同じアクセス権限になります。

＊ 本ソフトウェアでファイルを保護するためには、運用／使用する保護の形式に応じた権利ポリシーテンプレート(xml ファイル)が必要です。権利ポリシーテンプレートは、RMS サーバーや Azure RMS サーバー、もしくは FileShell クライアント設定からエクスポートされたものを使用してください。

＊ 権利ポリシーテンプレートをインポートした後は、その権利ポリシーでの保護を使用しなくなるまでは、権利ポリシーテンプレートの移動、削除、名前の変更などの操作は行わないでください。
ファイルの保護は、この権利ポリシーテンプレートを参照して行われるため、これらの操作をおこなった場合、保護に失敗する場合があります。

＊ 本ソフトウェアでは、権利ポリシーテンプレートの管理はおこないません。
権利ポリシーテンプレートの管理は、RMS サーバーの管理者、もしくは NFP 権利ポリシーの管理者がおこなってください。

＊ 既に保護されているファイルを、別の権利ポリシーテンプレートで保護しなおす(権限の付け替えをする)ことはできません。

＊ 本ソフトウェアでは、保護されたファイルの閲覧および保護解除はできません。
保護されたファイルの閲覧や保護解除の操作は、InfoCage FileShell クライアントなどを使用してください。
なお、本ソフトウェアをインストールしたサーバーマシンのエクスプローラー上では、保護されたファイルのアイコンに鍵マークは表示されません(InfoCage FileShell クライアントをインストールした PC のエクスプローラー上では、保護されたファイルのアイコンに鍵マークが表示されます)。

＊ 保護対象ファイルのパスにシンボリックリンクまたはジャンクションが含まれており、かつパス長が 8192 文字を超える場合は、ファイルを保護することはできません。
ファイルを保護する場合は、リンクを含まない実体のパスを指定する必要があります。

＊ 保護前に設定していた読み取り専用や隠しファイルなどのファイル属性が、保護時に外れる場合があります。保護後にファイル属性を再設定してください。

＊ 保護されたファイルのアーカイブビットの属性は引き継ぎます。また、圧縮属性・暗号化属性の属性は引き継ぎません。

＊ ファイルサーバーの「最終アクセス日時の更新」設定が有効、かつ保護対象ファイルが存在するディスクのファイルシステムが NTFS である場合、本ツールから同じファイルに対して何度も保護を実行すると、ファイルのアクセス日時が更新される場合があります。

＊「最終アクセス日時の更新」設定の状態は、下記手順で確認することができます。
1) コマンドプロンプトを「管理者として実行」で起動します。
2) 以下のコマンドを実行します。
fsutil behavior query disablelastaccess
3) 値が 0 の場合は、「最終アクセス日時の更新」設定が有効です。
値が 1 の場合は、「最終アクセス日時の更新」設定が無効です。

＊ ファイルサーバーにて OS のデータ重複除去機能を利用している環境で、この機能により最適化されているファイルに対してプロテクタ for NIAS による保護をおこなうと、重複除去が解除され、ディスク容量を消費します。大量のファイルを保護する場合、ディスクの空き領域に十分ご注意ください。
なお、重複除去が解除されたファイルについては、再度最適化が試行されます。

＊ ファイルサーバーにて OS のデータ重複除去機能を利用している環境で、FileShell による保護をおこなうと、エラーコード 0x80040307「ジャンクションまたはシンボリックリンクのファイルです。」でファイルの保護に失敗する場合があります。この場合、再度保護をおこなってください。

2.1.2 OfficeIRM/FileShell 形式の保護使用時の注意事項

＊ FileShell プロテクタ for NIAS で使用する FileShell SDK は、V6.1 より Azure RMS を利用して保護/保護解除をおこなう場合、対称鍵(Symmetric Key) による認証はできなくなりました。これに伴い、FileShell SDK V6.1 未満を使用している環境からアップデートする場合は、Azure RMS の認証をクライアントシークレットによる認証に変更する必要があります。

プロテクタ for NIAS のバージョンアップをおこなう前に、「3.4 MIP/Azure RMS を利用する場合に必要な情報の設定と取得」に記載の手順で、Azure Portal にてアプリケーションを登録し、クライアントシークレットの作成をおこなってください。

＊ MIP、もしくは Azure RMS を利用して保護/保護解除をおこなう場合に必要となるクライアントシークレットは、有効期限が切れた場合、Azure RMS の認証がおこなえなくなるため、運用年数やセキュリティリスクなどを考慮の上、適切な期限を設定し、運用中に期限が切れることのないよう管理をおこなってください。

クライアントシークレットの有効期限は、最大 24 か月です。
有効期限が切れた場合は、「3.4.3 クライアントシークレットの作成」に記載の手順でクライアントシークレットを再作成し、サーバ保護設定ツールに適用しなおしてください。

なお、クライアントシークレットが漏えいすると、Azure Active Diretory からユーザー・グループ・AU などの情報を第三者に取得される可能性があります。クライアントシークレットの管理には十分ご注意ください(漏えいの疑いがある場合は、すぐに Azure Portal でアプリの設定を無効化するなど、処置をおこなってください)。

＊ AD RMS サーバーを SSL で構築する場合、AD RMS のサーバー証明書は、自己署名証明書ではなく、信頼されたルート証明機関から発行された証明書を使用することを推奨します。評価環境等で自己署名証明書を使用する場合、本ソフトウェアを利用するためには、本ソフトウェアが動作するマシンのローカルコンピューターの信頼されたルート証明機関に、AD RMS サーバーのサーバー証明書(自己署名証明書)をインストールする必要があります。

＊ オンプレミスの RMS サーバーを使用する場合、本ソフトウェアをインストールしたサーバーマシンは、RMS サーバーと同一ドメインに属している必要があります(信頼関係で結ばれた異なるドメイン間での運用はできません)。

＊ 以下の拡張子をもつファイルは、OfficeIRM 形式で保護した後のファイルサイズが 2.0GB 以上となる場合、OS 仕様により保護に失敗します。

・Microsoft Office 形式のファイル
doc、dot、xla、xls、xlt、pps、ppt、pot、docm、docx、dotm、dotx、xlam、xlsb、xlsm、xlsx、xltm、xltx、xps、potm、potx、ppsx、ppsm、pptm、pptx、thmx、

・Microsoft Visio 形式のファイル
vsdx、vstx、vsdm、vstm

＊ FileShell 形式で保護されるファイルについて、ファイルパスが 260 文字以上、かつ、ファイルを保護した後のファイルサイズが 2GB(※)を超えるときは、対象のファイルを保護することができません。ファイルパスが 259 文字以内となる場所にファイルを移動してから保護してください。

(※)保護前のファイルサイズが、およそ 1.8GB 前後とお考えください。

＊ Mircosoft Office 形式の拡張子については、前述の注意事項を参照してください。
＊ Microsoft Visio 形式のファイル(vsdx、vstx、vsdm、vstm)を FileShell 形式で保護したファイルは、本注意事項に該当します。

＊ ファイルを保護した際、使用ライセンス(End User License:EUL)と呼ばれるファイルが OS によって作成されます。EUL ファイルは、ファイル保護がおこなわれるたびに蓄積されていき、ディスク使用量の消費につながるため、これらを利用しない場合には定期的に削除することをおすすめします。
なお、本ソフトウェアでは、ファイル保護をおこなった以降、EUL ファイルを使用することはありません。

EUL ファイルは以下のフォルダーに作成されます(「EUL」から始まる、拡張子が「.drm」のファイルが対象です)。

%allusersprofile%¥Microsoft¥MSIPC¥Server¥<SID>

＊ <SID>には、本ソフトウェアを動作させる時に使用するアカウントのものが入ります。
SID の確認は、本ソフトウェアを動作させる時に使用するアカウントでログオンし、コマンドプロンプトから、「whoami /user」コマンドを実行します。
コマンドの詳細については、「whoami /?」を実行してください。

2.1.3 Microsoft 互換/FileShell(ラベル)形式の分類/保護使用時の注意事項

＊ Microsoft Purview コンプライアンス ポータルや Auzre Portal に接続するためにプロキシサーバーの設定が必要なネットワーク環境の場合、保護、および保護解除するアカウントにプロキシサーバーの設定が適用されている必要があります。

詳細は以下のリンク先の情報を参照してください。
https://docs.microsoft.com/ja-jp/windows-server/administration/windows-commands/bitsadmin-util-and-setieproxy

2.1.4 NFP 形式の保護使用時の注意事項

＊ FileShell クライアントがバージョン 4.0 未満の場合、FileShell クライアント側で NFP 形式のファイルを閲覧・編集することはできません。

＊ サーバー認証版 NFP 権利ポリシーテンプレートで保護された NFP 形式のファイルを閲覧・編集するには、V6.1 以上の FileShell クライアントが必要です。

＊ NFP 権利ポリシーを使用して保護できるファイルのサイズは、4GB までとなります。4GB を超えるファイルを保護しようとした場合、エラーとなり保護することはできません。

第3章 FileShell プロテクタ for NIAS のインストール

3.1 運用環境構築の流れ

FileShell プロテクタ for NIAS の運用環境は、以下の手順で構築します。

No.	項目	内容	参照
1	必要なソフトウェアのインストール	FileShell プロテクタ for NIAS の利用に必要なソフトウェアをインストールします。	3.2
2	オンプレミスの RMS サーバー接続に必要な設定および情報の取得	FileShell プロテクタ for NIAS を使用するサーバーマシンがオンプレミスの RMS サーバーに接続するために必要な設定および情報の取得をおこないます。 ＊ NFP 形式のみを使用する場合は不要です。 ＊ MIP による分類/保護を利用する場合は不要です。	3.3
3	MIP による分類/保護の利用に必要な設定および情報の取得	プロテクタ for NIAS で MIP による分類/保護を利用するために必要な設定、および情報の取得をおこないます。 ＊ NFP 形式のみを使用する場合は不要です。 ＊ オンプレミスの RMS サーバーを利用する場合は不要です。	3.4
4	権利ポリシーテンプレートの準備	ファイルの保護に使用するポリシーテンプレートを準備します。	3.5
5	インストールの実行	FileShell プロテクタ for NIAS のインストールを実行します。	3.6
6	RMS サーバーの接続設定	環境設定ツールで RMS サーバーの接続設定をおこないます。 ＊ NFP 形式のみを使用する場合は不要です。	3.7
7	権利ポリシーテンプレートのインポート	ファイルの保護に使用する権利ポリシーテンプレートを FileShell プロテクタ for NIAS で使用できるよう、サーバーマシンにインポートします。	3.8

3.2 必要なソフトウェアのインストール

FileShell プロテクタ for NIAS を構築するには、以下のソフトウェアのインストールが必要です。
利用環境に各ソフトウェアがインストールされていない場合には、手順にしたがってインストールを実行してください。

＊ 動作環境に記載された URL からダウンロードを実行し、インストールしてください。

参照 ダウンロード URL については、「1.3 動作環境について」を参照してください。

- Visual Studio 2015、2017、2019、および 2022 用 Visual C++再頒布可能パッケージ
  - ＊ 64bit(x64)用モジュールをインストールしてください。
- RMS Client 2.1
  - ＊ OfficeIRM 形式、または FileShell 形式で保護する場合に必要です(NFP 形式のみを使用する場合は不要です)。

Windows Server 2016 および Windows StorageServer 2016 をご利用の場合は、以下のソフトウェアを動作環境に記載された URL からダウンロードし、インストールしてください

- Microsoft .NET Framework 4.7.2
  - ＊ Windows Server 2019、2022 をご利用の場合は、上記と同じか、より新しいバージョンの.NET Framework が OS のデフォルトでインストールされていますので、削除しないでください。
  - ＊ ご利用の OS と同じ言語の.NET Framework Language Pack を併せてインストールしてください。
  - ＊ Microsoft 社から提供される最新セキュリティパッチを適用してください。

3.3 オンプレミスの RMS サーバーへの接続に必要な設定

FileShell プロテクタ for NIAS でオンプレミスの RMS サーバーを利用する場合は、接続のために以下の設定が必要です。

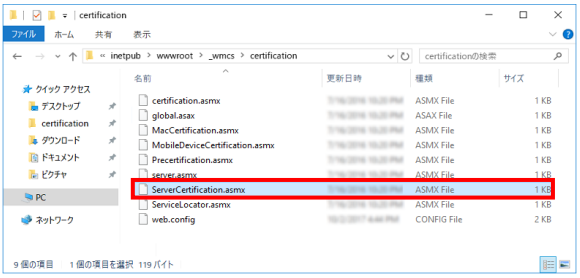
＊ MIP による分類/保護を利用する場合は、本節の設定は必要ありません。

＊ NFP 形式の保護のみを使用する場合は、本節の設定は必要ありません。

3.3.1 RMS 証明パイプラインに権限を追加する

FileShell プロテクタ for NIAS からオンプレミスの RMS サーバーに要求をするためには、RMS サーバーの RMS 証明パイプラインに FileShell プロテクタ for NIAS を使用するサーバーマシンのコンピューター名、および、AD RMS Service Group を追加する必要があります。

＊ 本設定はオンプレミスの RMS サーバーを使用する際に必要です。
Azure RMS を利用する場合、本設定は必要ありません。



RMS サーバーにて、ServerCertification.asmx ファイル※1 のアクセス許可に、FileShell プロテクタ for NIAS を実行するアカウント、および、AD RMS Service Group※2 を、”読み取りと実行”の権限で追加します。

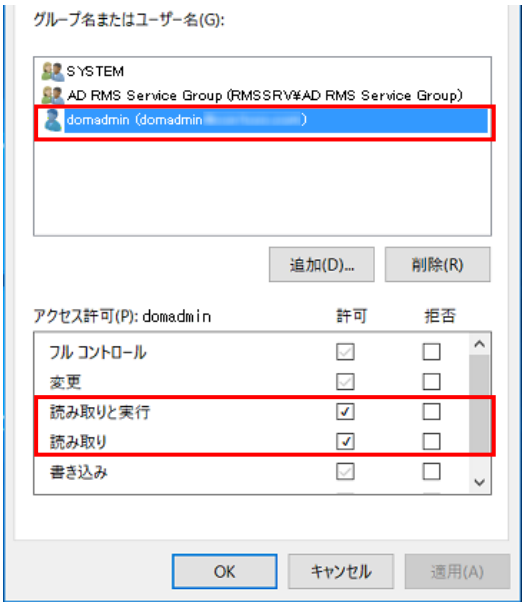
（※1）ServerCertification.asmx の既定のファイルパスは以下です。

%systemdrive%¥Inetpub¥wwwroot¥_wmcs¥Certification¥ServerCertification.asmx

＊ certification.asmx という別のファイルもあるため、間違えないようにご注意ください。

（※2）AD RMS Service Group は AD RMS サーバーのインストール時に作成されるセキュリティグループです。

例） FileShell プロテクタ for NIAS を実行するアカウントが domadmin の場合



RMS サーバーでの設定は以上です。

3.4 MIP/Azure RMS を利用する場合に必要な情報の設定と取得

プロテクタ for NIAS で MIP による分類/保護を利用するには、Azure Portal、および FileShell 付属の「Azure RMS 接続情報取得ツール」での情報設定とその取得が必要です。

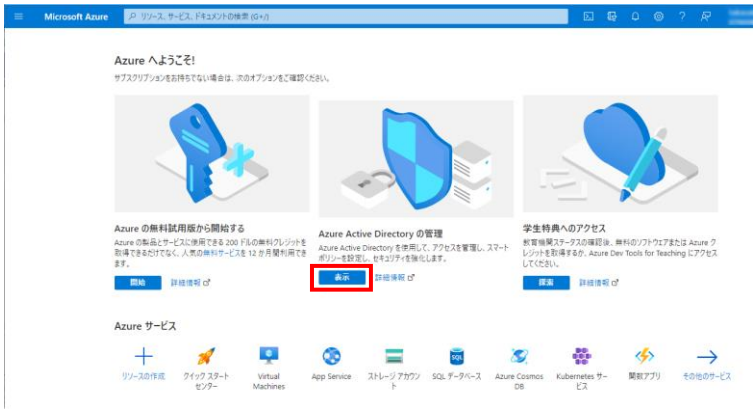
* 複数のサーバーマシンで本ソフトウェアを利用する場合でも、すべてのサーバーマシンで本節の手順を実行する必要はありません。
* V6.1 未満のプロテクタ for NIAS で、Azure RMS を利用している環境からアップデートする場合も、本項の手順を実施してください。
* オンプレミスの RMS サーバーを使用する場合は、本節の手順は必要ありません。
* NFP 形式の保護のみを利用する場合は、本項の手順は必要ありません。
* 「Azure RMS 接続情報取得ツール」は、64bitOS 環境のみで動作します。
* 「Azure RMS 接続情報取得ツール」は、FileShell クライアントがインストールされていない環境でも動作します。

3.4.1 Azure Portal でのアプリケーションの登録

Operation

1. Microsoft Azure portal (https://portal.azure.com) にアクセスし、テナントのグローバル管理者の資格情報を持つユーザーでログインします。

2. Azure portal ホームの「Azure Active Directory の管理」の[表示]をクリックします。



3. Azure Active Directory の管理で、メニューの[追加]から[アプリの登録]を選択します。

4. アプリケーションの登録で以下を入力/選択します。

- 名前:
  任意の名前を入力します(本書では"FileShell SDK"と入力することとします)。
- サポートされているアカウントの種類:
  [この組織のディレクトリのみに含まれるアカウント("テナント名"のみ-シングルテナント)]を選択します。
- リダイレクト URI:
  パブリック クライアント/ネイティブ(モバイルとデスクトップ)を選択し、入力欄には"fileshell://authorize"と入力します。
  ＊ 設定したリダイレクト URI は、プロテクタ for NIAS のインストーラー作成時に、プロパティ"ADAL_URI"に設定する値として使用します。

すべての入力/選択が完了後、[登録]をクリックします。

5. アプリケーションが登録されます。表示されるアプリケーションの情報のうち、以下の情報は、FileShell SDK のインストーラー作成時に使用します。

・アプリケーション(クライアント)ID ：プロパティ"ADAL_ID"に設定する値として使用します。

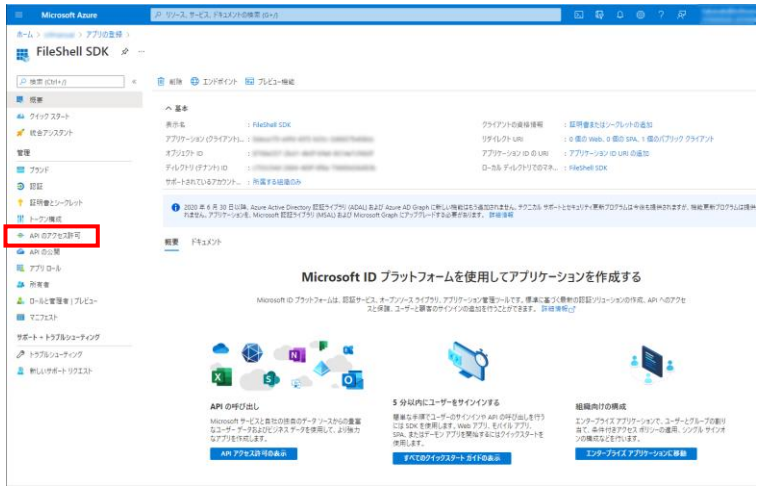
・ディレクトリ(テナント)ID ：プロパティ"ADAL_TENANT_ID"に設定する値として使用します。

以上で、アプリケーションの登録は終了です。引き続き、「3.4.2 API アクセス許可の追加」を実施してください。

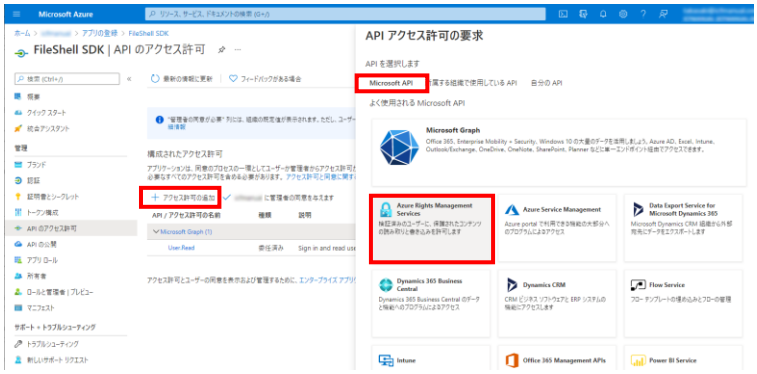
3.4.2 API アクセス許可の追加

Operation

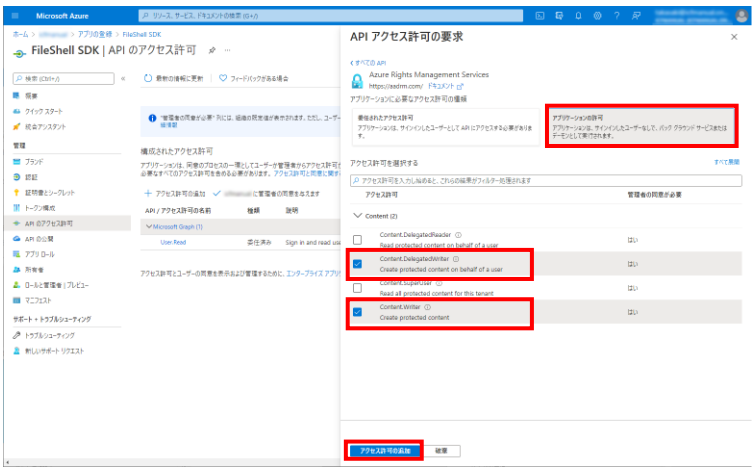
1. 登録したアプリケーションの画面の左メニューの[管理]から[API のアクセス許可]をクリックします。



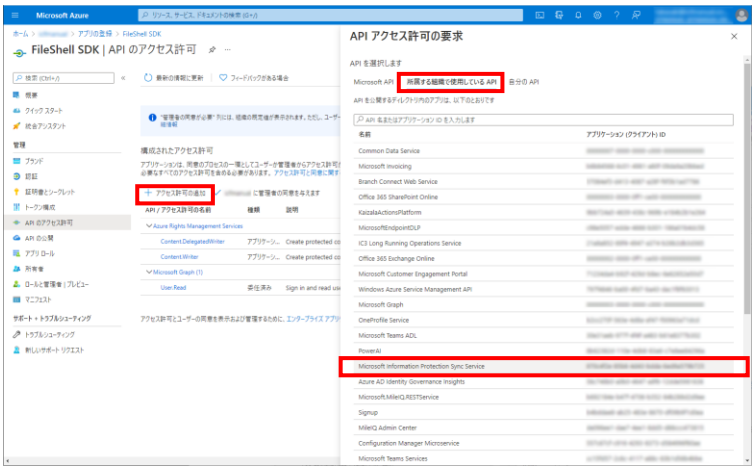
2. API アクセスの許可の要求で、[アクセス許可の追加]をクリックすると表示される「API アクセス許可の要求」で、[Microsoft API]の[Azure Rights Management Service]を選択します。



3. API のアクセス許可要求で[アプリケーションの許可]を選択し、[Content.DelegatedWriter] と、[Content.Writer]にチェックを入れて、[アクセス許可の追加]をクリックします。

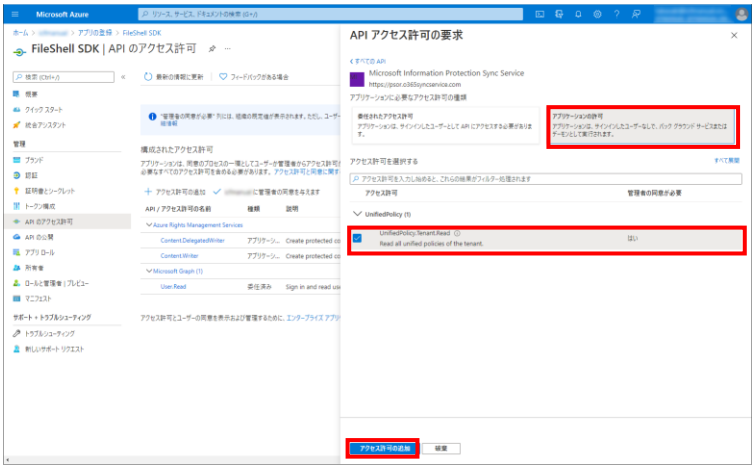


4. 手順 **3** で追加したアクセス許可が追加されたことを確認したのち、もう一度[アクセス許可の追加]をクリックし、API アクセス許可の[所属している組織で使用している API]を選択し、表示される一覧から、[Microsoft Information Protection Sync Service]を選択します。

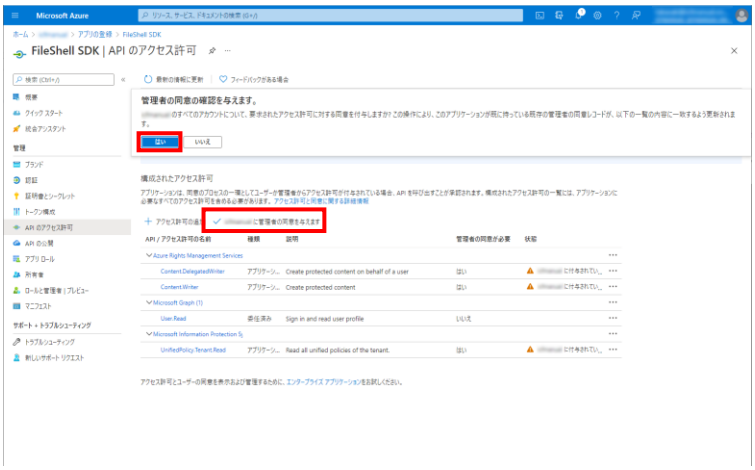


＊ 一覧に[Microsoft Information Protection Sync Service]が表示されていない場合は、一覧下部の[さらに読み込む]をクリックしてください。

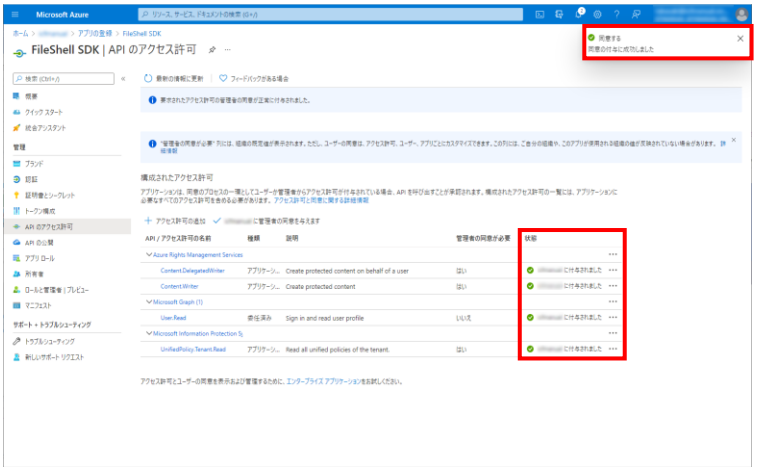
5. API のアクセス許可要求で[アプリケーションの許可]を選択し、[UnifiedPolicy.Tenant.Read]にチェックを入れて、[アクセス許可の追加]をクリックします



6. 手順 **5** で追加したアクセス許可が追加されたことを確認したのち、[(テナント名)の管理者に同意を与えます]をクリックすると、「管理者の同意の確認を与えます。」のメッセージが表示されますので[はい]を選択します。



7. 同意の付与に成功するとメッセージが表示され、構成されたアクセス許可の状態が更新されます。

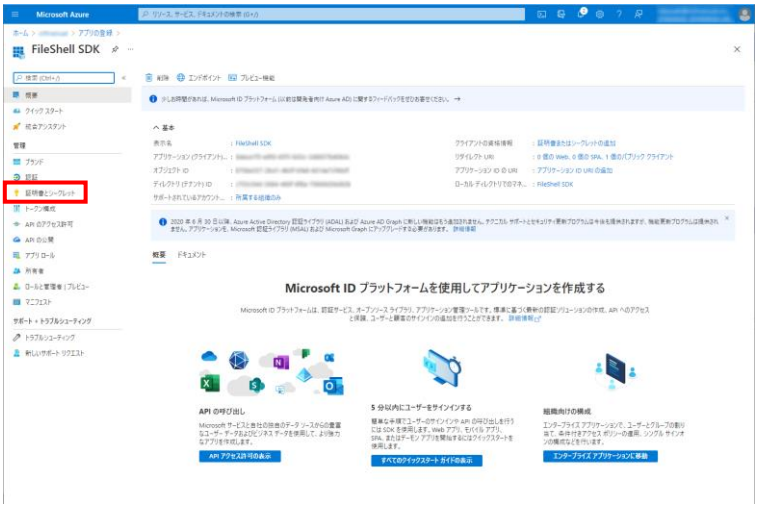


以上で、アプリケーションへの API のアクセス許可の追加は終了です。引き続き「3.4.3 クライアントシークレットの作成」を実施してください。

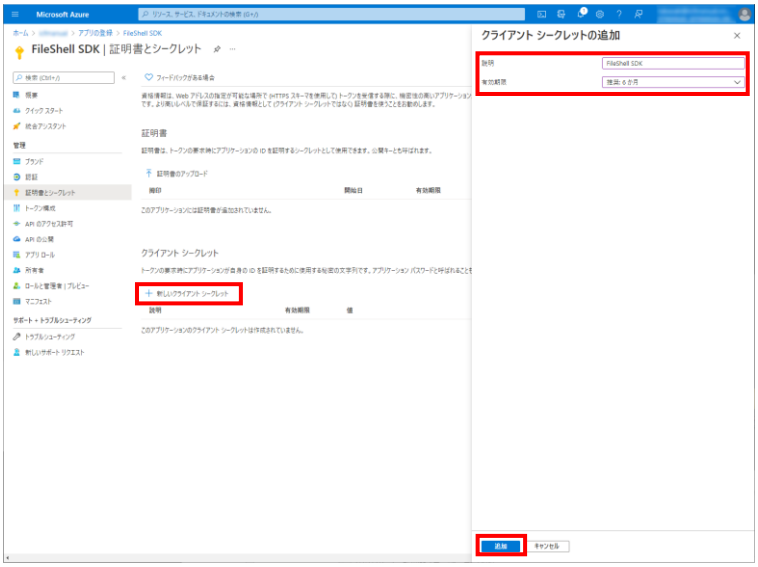
3.4.3 クライアントシークレットの作成

Operation

1. 登録したアプリケーションの画面で、左側のメニューの[管理]から[証明書とシークレット]をクリックします。



2. クライアントシークレットの[新しいクライアントシークレット]をクリックすると表示されるクライアントシークレットの追加で、[説明]と[有効期限]を設定し、[追加]をクリックします。



＊ クライアントシークレットの有効期限は最大 24 か月です。運用年数、セキュリティリスクなどを考慮の上、適切な期限を設定し、運用中に期限が切れることのないよう管理をおこなってください。有効期限が切れた場合は、本項に記載の手順でクライアントシークレットを再作成してください。

＊ クライアントシークレットが漏えいすると、Azure Active Diretory からユーザー・グループ・AU などの情報を第三者に取得される可能性があります。クライアントシークレットの管理には十分ご注意ください(漏えいの疑いがある場合は、すぐに Azure Portal でアプリの設定を無効化するなど、処置をおこなってください)。

3. アプリケーションの資格情報が正常に更新された旨のメッセージが表示され、クライアントシークレットが追加されますので、表示されている値を控えます。

＊ ここで表示されるクライアントシークレットの値は、あとから参照することができませんので、**表示されたタイミングで必ず控えるようにしてください。**

＊ 値が表示されている右側の アイコンをクリックすると、値をクリップボードにコピーできます。

以上で、クライアントシークレットの作成は終了です。

3.4.4 Azure RMS のライセンスサーバー、および認証サーバーURL の取得

Azure RMS のライセンスサーバー、および認証サーバーURL の取得方法は以下のとおりです。

Operation

1. Windows PowerShell から、本操作に必要となるモジュールをインストールします。
Windows の[スタートメニュー]からプログラムの一覧を表示し、[Windows PowerShell]の右クリックメニューから、「管理者として実行」を選択します。

2. 以下のコマンドを実行し、TLS1.2 を有効にします。

> [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bOR [Net.SecurityProtocolType]::Tls12

お使いの環境が Windows Server 2019 以降の場合は、本コマンドの実行は不要です。

3. 以下のコマンドを実行し、次のモジュールをインストールします。

AIPService PowerShell モジュール

> Install-Module -Name AIPService

＊ お使いの環境に Azure Rights Management Administration Tool (AADRM)がインストールされている場合は、以下のコマンドを実行し、AADRM をアンインストールしてから AIPSevice PowerShell モジュールをインストールしてください。

> Uninstall-Module -Name AADRM

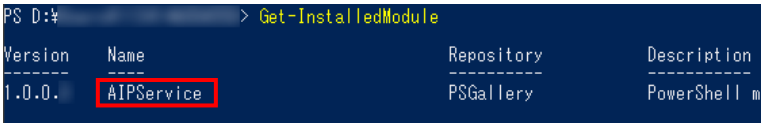
＊ パッケージマネージャー「nuget」のインストール確認メッセージが表示された場合は、「Y」を入力して続行してください。

＊ モジュールのインストール時に、「信頼されていないリポジトリからモジュールをインストールしようとしています。..」と表示された場合は、「Y」を入力して続行してください。

4. 以下のコマンドを実行し、モジュール一覧を取得します。

> Get-InstalledModule

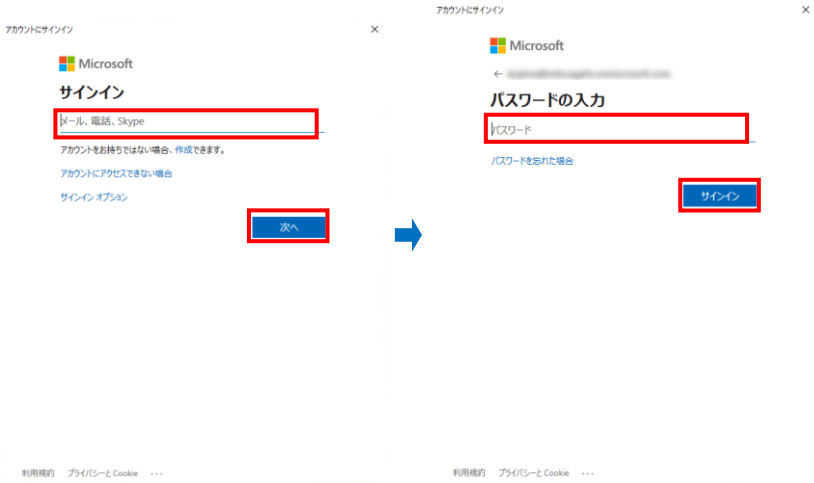
5. 一覧の「Name」に手順 *3* でインストールしたモジュールが表示されていることを確認します。



6. 以下のコマンドを実行します。

> Connect-AIPService

7. 表示されたサインイン画面で Azure のユーザーID とパスワードを入力し、サインインします。

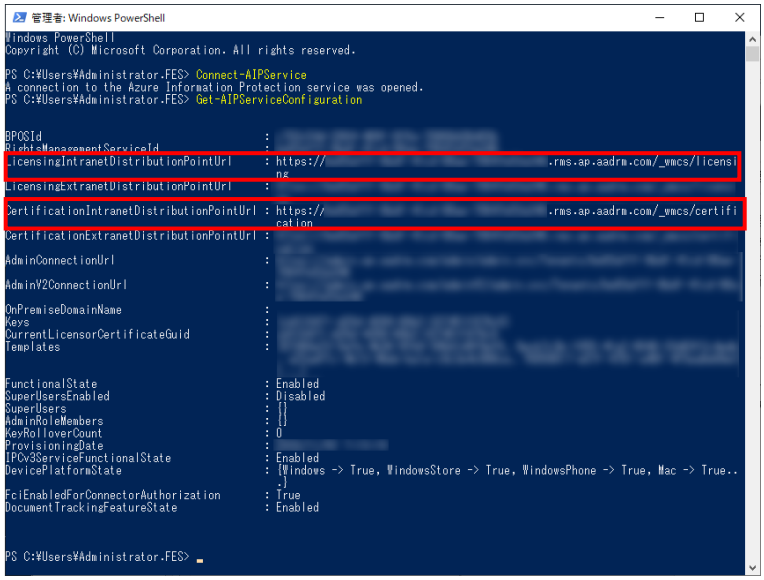


＊ グローバル管理者の資格情報を持つユーザーで接続してください。

8. 以下のコマンドを実行します。

> Get-AIPServiceConfiguration

9. 表示された「LicensingIntranetDistributionPointUrl」(Azure RMS のライセンスサーバーURL)、および「CertificationIntranetDistributionPointUrl」(Azure RMS の認証サーバーURL)を確認します。



本手順で取得した Azure RMS のライセンスサーバーURL、および認証サーバーURL は、「4.3 環境設定ツールの操作」－「4.3.1 RMS 認証情報設定」で使用します。

3.5 権利ポリシーテンプレートの準備

FileShell プロテクタ for NIAS で、OfficeIRM/FileShell 形式または NFP 形式でファイルを保護するためには、運用／使用する保護の形式に応じた権利ポリシーテンプレート(xml ファイル)が必要です。

権利ポリシーテンプレートは、RMS サーバーや Azure RMS サーバー、もしくは FileShell クライアント設定からエクスポートされたものを使用してください。

以下に権利ポリシーテンプレートの取得および保存方法について、運用形態ごとに例をあげて説明します。
保存した権利ポリシーテンプレートは、「3.8 権利ポリシーテンプレートのインポート」で使用します。

＊ MIP による分類/保護のみを利用する場合は、権利ポリシーテンプレートを使用しませんので、本節の手順をおこなう必要はありません。

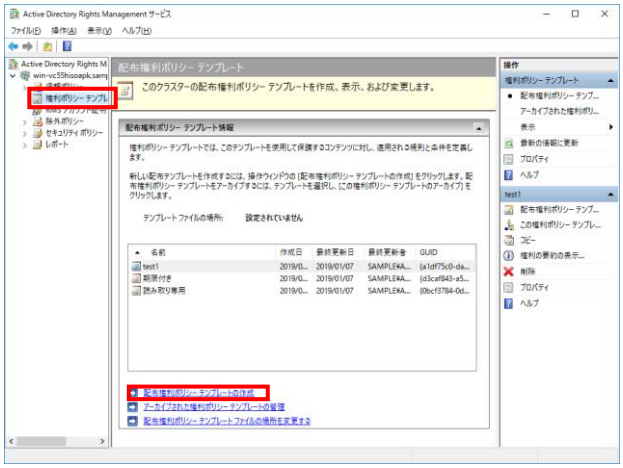
＊ 本ソフトウェアでは、権利ポリシーテンプレートの管理はおこないません。
権利ポリシーテンプレートの管理は、RMS サーバーの管理者、もしくは NFP 権利ポリシーの管理者がおこなってください。

3.5.1 オンプレミス RMS サーバー上の権利ポリシーテンプレートの取得と保存

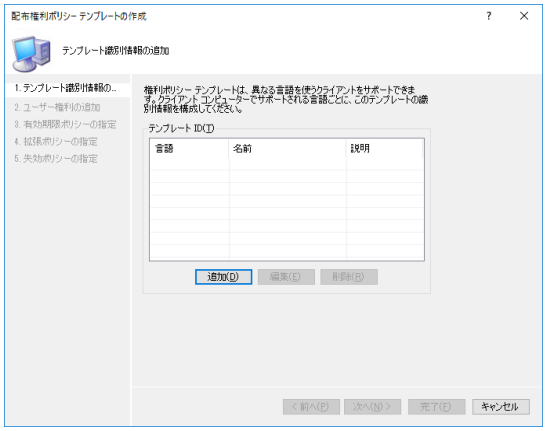
オンプレミスの RMS サーバーから権利ポリシーテンプレートを XML ファイル形式で保存する方法を説明します。

Operation

1. Active Directory Rights Management サービスの左部のツリーから「権利ポリシーテンプレート」を選択し、下部に表示される「配布権利ポリシーテンプレートの作成」を選択します。



2. 下記の配布権利ポリシーテンプレートの作成で表示されるダイアログに従い、テンプレート名、アクセスユーザーおよびアクセス権限、保護ファイルの有効期限等を必要に応じて指定して、権利ポリシーテンプレートを作成します。作成した権利ポリシーテンプレートは「テンプレートファイルの場所」で指定されたパスに出力することができます。



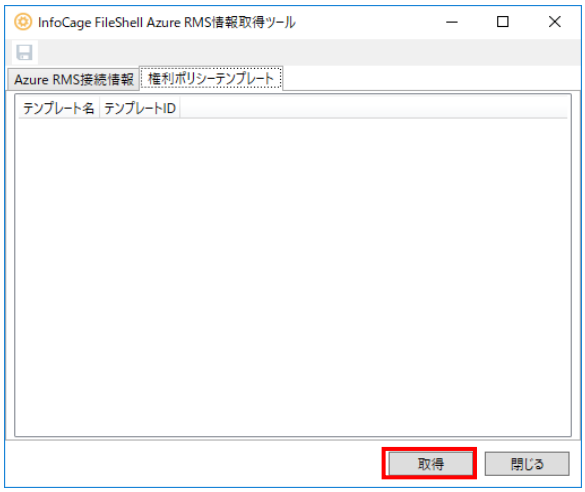
3.5.2 Azure RMS サーバー上の権利ポリシーテンプレートの取得と保存

「Azure RMS 接続情報取得ツール」を使用して、Azure RMS サーバー上の権利ポリシーテンプレートを XML ファイル形式で保存する方法を説明します。

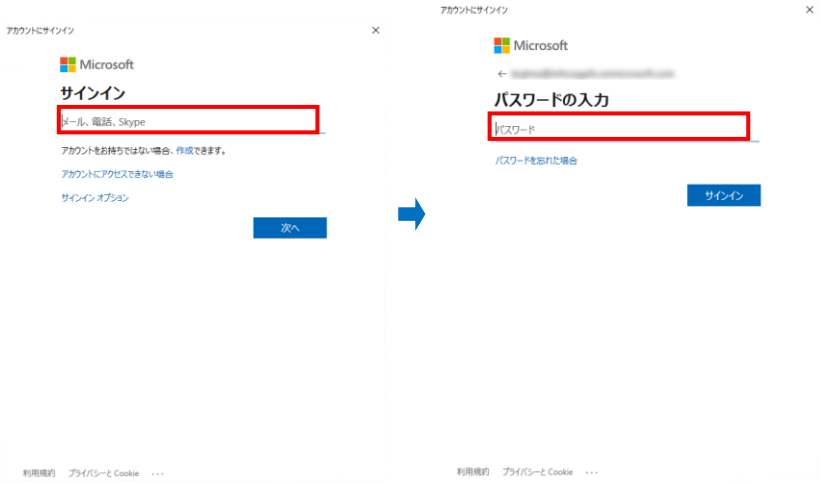
参照 「Azure RMS 接続情報取得ツール」のインストール方法については、『管理者ガイド』の「Azure RMS 接続情報取得ツールの導入手順」を参照してください。

Operation

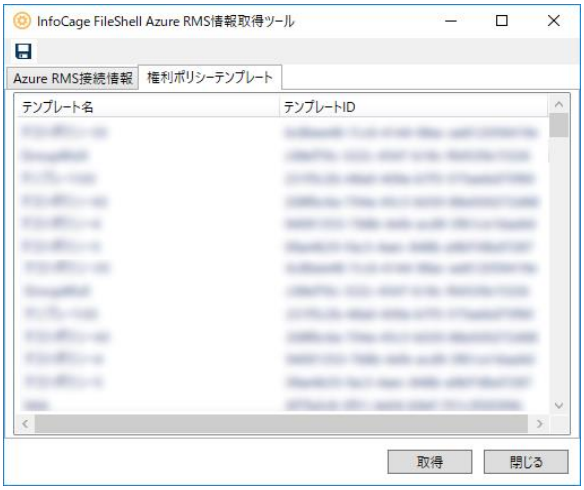
1. C:¥ IcfGetAzureInfo から、「IcfGetAzureInfoTool.exe」を起動します。
2. [権利ポリシーテンプレート]タブをクリックします。
3. テンプレート一覧画面が表示されます。
   [取得]をクリックします。



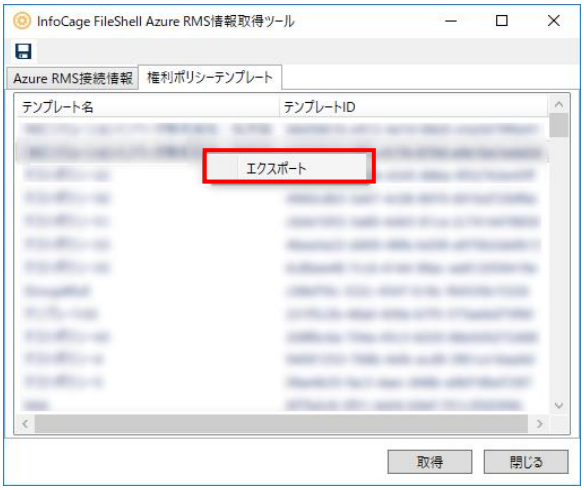
4. サインイン画面が表示された場合は、Azure のユーザーID とパスワードを入力します。



5. テンプレート一覧画面に Azure RMS サーバー上の権利ポリシーテンプレートの情報が表示されます。



6. 対象の権利ポリシーテンプレートを右クリックして、[エクスポート]を選択します。



7. 保存ダイアログでファイル名を入力し、[保存]をクリックします。

＊ 画面左上の は、権利ポリシーテンプレートの保存には使用できません。

以上で、Azure RMS サーバー上の権利ポリシーテンプレートの取得および保存は完了です。

3.5.3 NFP 権利ポリシーテンプレートの取得と保存

FileShell サーバーから NFP 権利ポリシーテンプレートを XML ファイル形式で保存する方法を説明します。

参照 *NFP 権利ポリシーテンプレートの詳細については、『NEC File Protection Edition 管理者ガイド』、もしくは『NEC File Protection Edition 利用ガイド』を参照してください。

Operation

1. FileShell サーバーに全体管理者もしくは組織管理者でログインし、Web 管理コンソールの組織管理者用画面で「ラベル/権利ポリシ管理」を選択します。

2. 権利ポリシー一覧に表示されている「NFP 権利ポリシーテンプレート情報」から利用する NFP 権利ポリシーテンプレートの右部[操作]メニューでエクスポートを選択し「実行」をクリックします

3. エクスポート画面が表示されます。

＊ 利用する NFP 権利ポリシーテンプレートにより、保存の方法が異なります。

サーバー認証版の NFP 権利ポリシ―テンプレートの場合

識別情報を必要に応じて追加・編集後、インポート時に使用するパスワードを設定し[実行]をクリックして出力される NFP 権利ポリシーファイル(xml ファイル)を保存します。

＊ 識別情報以外の設定は、エクスポート時に任意に設定することはできません(各設定項目はグレーアウトされ、選択／入力できません)。

＊ 利用権限の「所有者(作成者)に無期限のフルコントロールの権利を付与する」設定、および有効期限の設定は、エクスポートしようとする権利ポリシーテンプレートに設定された内容が引き継がれます。

＊ 利用権限のうち、「所有者(作成者)に無期限のフルコントロールの権利を付与する」を除く設定は、OFF の状態となります(これらは、保護されたファイルを開く際に、FileShell サーバーにアクセスして、確認されます)。

鍵配布版の NFP 権利ポリシーテンプレートの場合

付与する識別情報、利用権限、有効期限およびインポート時に使用するパスワードを設定後、[実行]ボタンをクリックして出力される NFP 権利ポリシーファイル(xml ファイル)を保存します。

以上で、鍵配布版の NFP 権利ポリシーテンプレートの取得および保存は終了です。

3.6 FileShell プロテクタ for NIAS のインストール

FileShell プロテクタ for NIAS のインストールは以下の手順で実行してください。

3.6.1 インストールパッケージの展開

FileShell プロテクタ forNIAS の運用環境を構築するために必要なインストールパッケージは、以下の手順で展開してください。

Operation

1. InfoCage FileShell の CD-ROM から、本ソフトウェアをインストールするサーバーマシンの任意のフォルダーに、FileShell プロテクタ for NIAS (¥ProtectorForNIAS) をフォルダーごとコピーします。
本書では、「D:¥ProtectorForNIAS」としてコピーしたと仮定します。

■ **CD-ROM 内 フォルダー構成**

フォルダー名	説明
¥Tools	
└¥ProtectorForNIAS	FileShell プロテクタ for NIAS モジュール格納フォルダー
├SDK	InfoCage FileShell SDK 格納フォルダー
├x64	64bit 用インストールパッケージ格納フォルダー
├Product.ini	モジュール情報ファイル
├Setup.exe	インストール実行ファイル
└Setup.ini	インストール設定ファイル

配置イメージ

[D:¥ProtectorForNIAS]フォルダー配下に、[Setup]フォルダー配下一式を配置します。

D:¥ProtectorForNIAS
└¥ProtectorForNIAS

2. メディアキット CD-ROM から、インストーラ作成支援ツールのインストールの格納フォルダー(¥Tools¥SetupConfig) を PC の任意のフォルダーにコピーしてください。本書では、「D:¥ProtectorForNIAS」にコピーしたと仮定します。

配置イメージ

[D:¥ProtectorForNIAS]フォルダー配下に、[Setup]フォルダー配下一式を配置します。

D:¥ProtectorForNIAS
├ ¥ProtectorForNIAS(手順 *1* で配置したフォルダー)
└ ¥SetupConfig

以上で、インストールパッケージの展開は終了です。

3.6.2 NFP の緊急保護解除用の公開鍵の取得

＊ NFP 形式の保護を利用しない、または NFP の緊急保護解除機能を使用しない場合は、本項の手順は不要です。

NFP の緊急保護解除機能は、NFP 形式のファイルを保護した権利ポリシーを紛失した場合などに、緊急措置としてファイルの保護を強制的に解除するための機能です。FileShell SDK で NFP 形式の保護を利用する際は、NFP の緊急保護解除機能を有効にして使用することを推奨します。

FileShell SDK で NFP の緊急保護解除機能を有効にするには、インストール設定ファイルにて、緊急保護解除機能を有効にし、公開鍵を設定する必要があります。使用する権利ポリシーに応じて、以下の手順で公開鍵を事前に取得し、次項「3.6.3 インストーラーの設定」で、インストール設定ファイルに設定してください。

＊ 緊急保護解除機能が有効でない環境で保護された NFP 形式のファイルは、保護した権利ポリシーを紛失した場合、ファイルの保護を解除することができません。万一の場合に備え、本機能を有効にして利用することを推奨します。

＊ 緊急保護解除機能による保護解除については『NEC File Protection Edition 管理者ガイド』の「NFP の緊急保護解除機能による保護解除について」を参照してください。

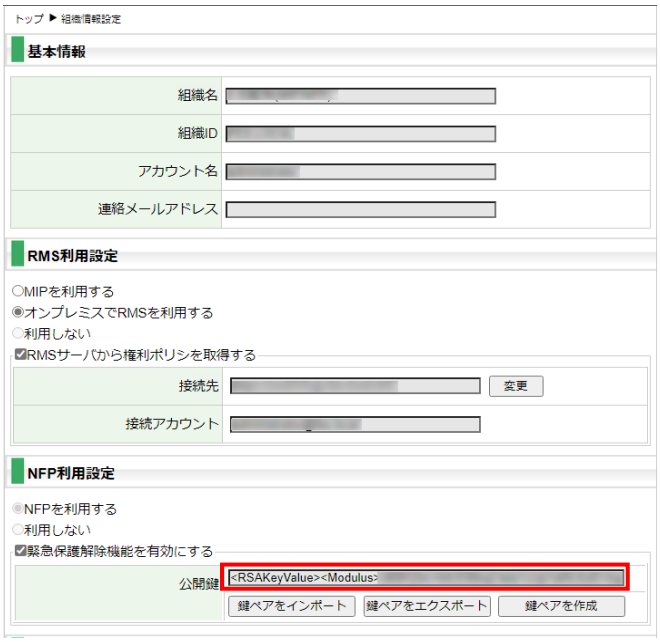
● FileShell サーバーで作成した NFP 権利ポリシーを使用する場合

Operation

1. FileShell サーバーに全体管理者もしくは組織管理者の ID でログインします。
2. [組織管理者用]メニューから[組織設定]をクリックします。

＊ 全体管理者の ID でログインした場合は[組織管理]-[組織一覧]から設定したい組織を選択することで、[組織管理者用]メニューを表示できます。

3. [組織情報設定]画面を開き、[権利ポリシ利用設定]の「公開鍵」に表示されている緊急保護解除用の公開鍵を取得します。[公開鍵]に表示されている文字列をコピーしてご使用ください。



＊ 公開鍵が作成されていない場合は、「鍵ペアを生成」ボタンで公開鍵を生成してください。

● FileShell クライアントで作成した NFP 権利ポリシーを使用する場合

Operation

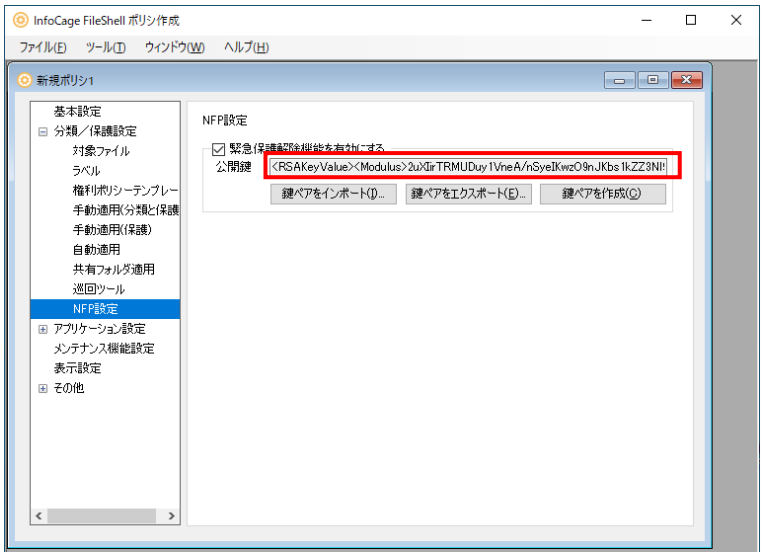
1. NFP 権利ポリシーを作成した FileShell クライアントがインストールされている環境で、コマンドプロンプトでカレントを FileShell クライアントのインストール先に移動し、以下のコマンドを実行します。

IcfClientSetting.exe /CreatePolicy

＊ FileShell クライアントは、デフォルトでは以下にインストールされています。
〈システムドライブ〉¥Program Files¥NEC¥InfoCageFileShell¥

2. FileShell ポリシー作成画面が表示されます。サブのメニューツリーから[保護設定]-[NFP 設定]を選択し、表示されている[公開鍵]を取得します。

＊ 公開鍵が作成されていない場合は、[鍵ペアを作成]ボタンで公開鍵を作成してください。



以上で NFP の緊急保護解除用の公開鍵の取得は終了です。

3.6.3 インストーラーの設定

利用する保護形式に応じたインストーラーの設定をおこないます。

インストーラーの設定は、インストーラ作成支援ツールでおこないます。

＊ インストーラーの設定は必ずインストーラ作成支援ツールを使用しておこなってください。テキストエディタ等によるインストーラー設定ファイルの編集はおこなえません。

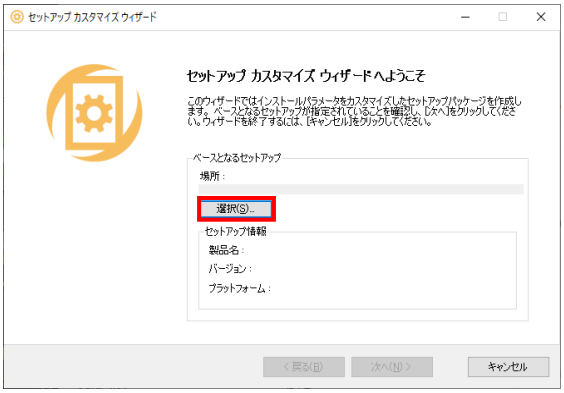
＊ インストーラ作成支援ツールについての詳細は、『インストールガイド』の「インストーラ作成支援ツール」を参照してください。

＊ 本項の手順では、「3.6.1 インストールパッケージの展開」に記載の配置イメージどおりにインストールパッケージを展開したものとして説明しています。インストールパッケージの配置フォルダーを変更している場合は、変更したフォルダーに読み替えて手順をすすめてください。

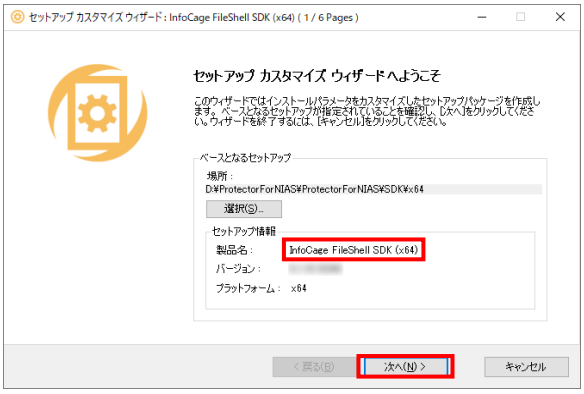
Operation

1. 「D:¥ProtectorForNIAS¥SetupConfig¥setupconfig.exe」を実行します。

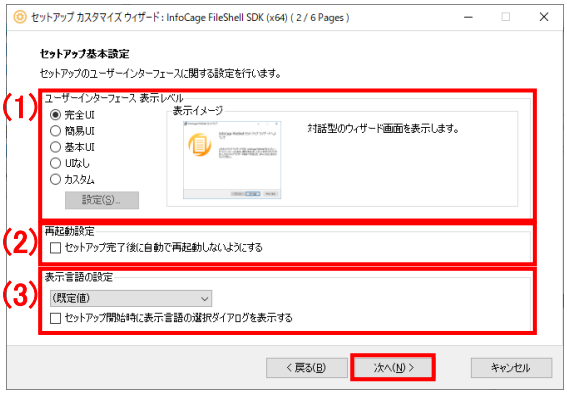
2. インストーラ作成支援ツールが起動し、「セットアップ カスタマイズ ウィザードへようこそ」画面が表示されます。［ベースとなるセットアップの情報］の［選択］ボタンをクリックし、「D:¥ProtectorForNIAS¥ProtectorForNIAS¥SDK¥x64¥Setup.exe」を指定します。



3. ［セットアップ情報］の［製品名］が、"InfoCage FileShell SDK (x64)"になっていることを確認し、［次へ］をクリックします。

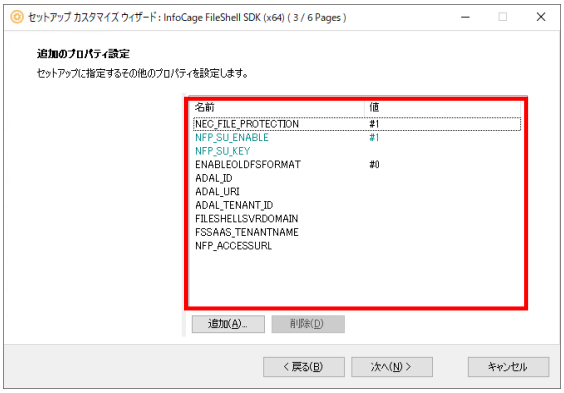


4. 「セットアップ基本設定」画面が表示されます。
以下の項目を必要に応じて設定し、[次へ]をクリックします。



項目		内容
(1)	ユーザーインタフェース表示レベル	UI の表示レベルを選択します。 サイレントインストールをおこなう場合は、[UI なし]を選択します。 ＊ その他の表示レベルについては、[表示イメージ]欄内の説明をご参照ください。
(2)	再起動設定	FileShell SDK のセットアップでは、自動で再起動はおこなわれないため、設定の必要はありません(チェックを入れなくても、OS の再起動はおこなわれません)。
(3)	表示言語の設定	セットアップ開始時に表示される言語をリストから選択します。 セットアップ開始時に表示言語の選択ダイアログを表示する場合は、チェックボックスにチェックを入れます。

5. 追加のプロパティ設定画面が表示されますので、利用する環境に応じた設定をおこないます。



プロパティ名をダブルクリックすると、プロパティの編集画面が表示されます。利用する形態に応じて以下の一覧を参考に、プロパティの[値のデータ]の編集をおこなってください。

＊ 画面上に表示されていないプロパティは[追加]ボタンで追加することができます。
＊ プロテクタ for NIAS で MIP による分類／保護を利用する場合は、以下のプロパティの設定が必要です。

・ ADAL_ID　「3.4.1 Azure Portal でのアプリケーションの登録」の手順 5 で取得した「アプリケーション(クライアント)ID」を指定してください。

・ ADAL_URI　「3.4.1 Azure Portal でのアプリケーションの登録」の手順 4 で設定した「リダイレクト URI」を指定してください。

・ ADAL_TENANT_ID　「3.4.1 Azure Portal でのアプリケーションの登録」の手順 5 で取得した「ディレクトリ(テナント) ID」を指定してください。

＊ 以下に該当する場合は、プロパティ"MSIPC_MSAL_ENABLE"を、設定値"#0"(MSIPC で MSAL での認証を使用しない)で追加してください。

・ オンプレミスの AD RMS のみを利用する場合

・ オンプレミスの AD RMS から Azure RMS に移行した環境で、対称鍵(Symmetric Key)による認証を利用したい場合

・ NFP のみを利用する場合

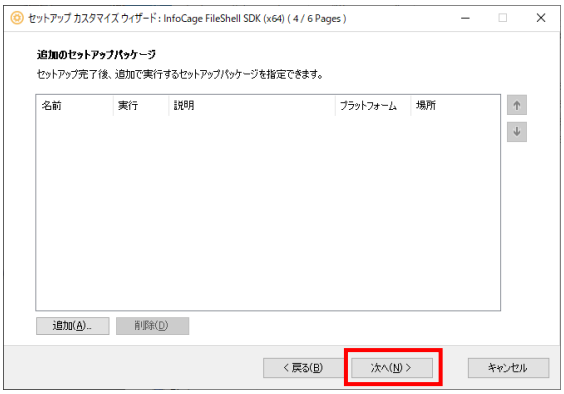
＊ NFP の緊急保護解除に関する設定については、「3.6.4 NFP の緊急保護解除に関する設定例」に、利用形態ごとの設定例を記載しておりますので、参考にしてください。

プロパティ名	内容	設定
NEC_FILE_PROTECTION	NFP 機能の有効／無効を設定します。	#0: 無効 #1: 有効(既定値)
NFP_SU_ENABLE	NFP の緊急保護解除機能を有効／無効を設定します。 ＊ 緊急保護解除機能が有効でない環境で保護された NFP 形式のファイルは、保護した権利ポリシーを紛失した場合、ファイルの保護を解除することができません。NFP 機能を利用する場合は、万一の場合に備え、本機能を有効にして利用することを推奨します。 ＊ 有効にする場合は、NFP_SU_KEY に、公開鍵文字列の設定が必要です。	#0: 無効 #1: 有効(既定値)
NFP_SU_KEY	NFP の緊急保護解除機能で使用する公開鍵文字列を指定します。	NFP の緊急保護解除機能を利用する場合:「3.6.2 NFP の緊急保護解除用の公開鍵の取得」で取得した公開鍵を、"文字列"形式で指定します。 NFP の緊急保護解除機能を利用しない場合:空欄とします。
ENABLEOLDFSFORMAT	V5.0 以前のクライアントと互換性のある FileShell 形式の保護を有効にします。(FileShell 形式有効設定) ＊ 本設定を有効に設定した場合、MIP による分類／保護をおこなってもラベルは付与されません。	#0 :無効(既定値) #1 :有効

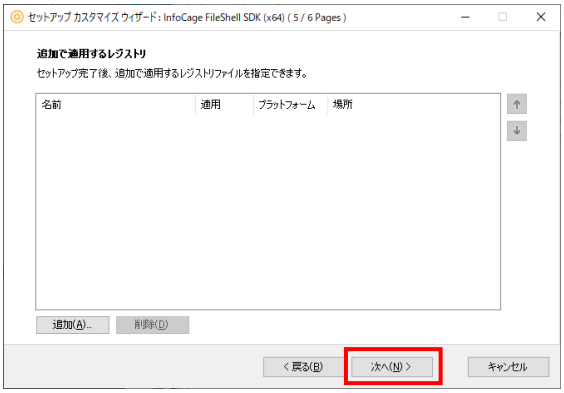
MSIPC_MSAL_ENABLE	MSIPC で MSAL での認証を使用する設定です。 本設定は、Azure RMS への認証を MSIPC で利用する場合に有効にします。 ＊ 以下に該当する場合は、本プロパティの設定を" #0"(MSIPC で MSAL での認証を使用しない)に設定してください。 ・オンプレミスの AD RMS のみを利用する場合 ・オンプレミスの AD RMS から Azure RMS に移行した環境で、対称鍵(Symmetric Key)による認証を利用したい場合 ・NFP のみを利用する場合	#0 ： MSIPC で MSAL での認証を使用しない #1 ： MSIPC で MSAL での認証を使用する(既定値)
ADAL_ID	MIP/Azure RMS を利用する場合に、「3.4.1 Azure Portal でのアプリケーションの登録」の手順 5 で取得した「アプリケーション(クライアント)ID」を指定します。	"文字列"形式で指定します。
ADAL_URI	MIP/Azure RMS を利用する場合に、「3.4.1 Azure Portal でのアプリケーションの登録」の手順 4 で設定した「リダイレクト URI」を指定します。	"文字列"形式で指定します。
ADAL_TENANT_ID	MIP/Azure RMS を利用する場合に、「3.4.1 Azure Portal でのアプリケーションの登録」の手順 5 で取得した「ディレクトリ(テナント)ID」を指定します。	"文字列"形式で指定します。
FILESHELLSVRDOMAIN	FileShell サーバーの組織設定にて、ID 配布方式でポリシの配布先を管理する組織を利用する場合に、その組織の組織 ID として設定しているドメイン名を指定します。	"文字列"形式で指定します。 ＊ 簡易配布でポリシの配布先を管理する組織を利用する場合は、本プロパティを設定しないでください。
FSSAAS_TENANTNAME	FileShell サーバーの組織設定にて、簡易配布でポリシの配布先を管理する組織を利用する場合に、その組織の組織 ID を指定します。	"文字列"形式で指定します。 ＊ ID 配布でポリシの配布先を管理する組織を利用する場合は、本プロパティを設定しないでください。
NFP_ACCESSURL	サーバー認証版の NFP 権利ポリシーで使用する FileShell サーバーの URL を指定します。 ＊ 本設定は、サーバー認証版の NFP 権利ポリシーテンプレートを使用する場合のみ必要です。 ＊ サーバー認証版の NFP 権利ポリシーテンプレートを使用する場合、本設定がおこなわれていないと保護することができません。	"文字列"形式で指定します。 ＊ http:// 、もしくは https://で始まる URL を指定ください。 ＊ スペース(全角、半角)を含む URL は指定できません。

設定完了後、[次へ]をクリックします。

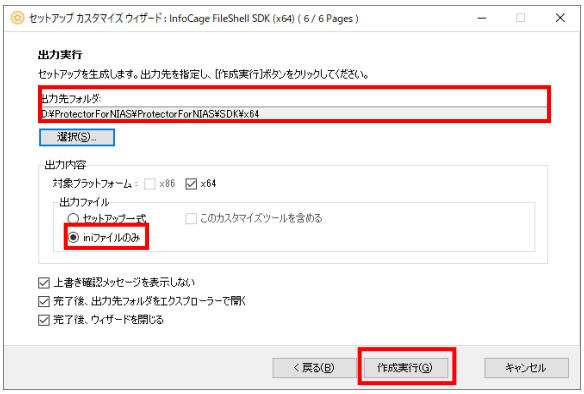
6. [追加のセットアップパッケージ]画面が表示されますので、[次へ]をクリックします。



7. [追加で適用するレジストリ]画面が表示されますので、[次へ]をクリックします。

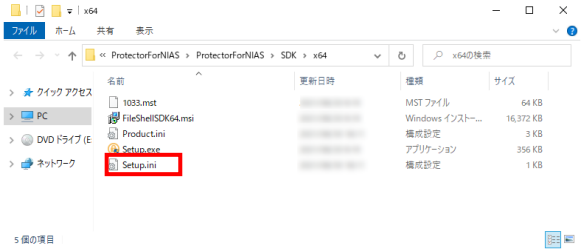


8. 「出力実行」画面が表示されます。[出力先フォルダ]に"D:¥ProtectorForNIAS¥ProtectorForNIAS¥SDK¥x64"を指定し、[出力内容]で[ini ファイルのみ]を選択して、[作成実行]をクリックします。



＊ 作成実行をクリックした際に、ファイルへのアクセスが拒否された旨のエラーメッセージが表示される場合は、出力先フォルダの setup.ini ファイルに読み取り専用属性が付与されている可能性があります。その場合は、読み取り専用属性を解除してから再度、作成実行をおこなってください。

9. 指定した出力先フォルダーに setup.ini ファイルが出力され、更新されます



＊ 出力される setup.ini ファイルには読み取り専用属性が付与されます。本項の手順で setup.ini ファイルを更新した後、同じフォルダの setup.ini ファイルを再更新する場合は、当該ファイルの読み取り専用属性を解除してください。

以上で、インストーラーの設定は終了です

3.6.4 NFP の緊急保護解除に関する設定例

NFP 形式の保護を利用しない場合の設定

プロパティ名	内容	値の設定
NEC_FILE_PROTECTION	NFP を無効に設定します。	#0 ＊[値のデータ]には#を入力しないでください。
NFP_SU_ENABLE	緊急保護解除機能を無効に設定します。	#0 ＊[値のデータ]には#を入力しないでください。
NFP_SU_KEY	空欄のままとします。	

NFP 形式の保護を利用する場合の設定（緊急保護解除機能有効）

プロパティ名	内容	値の設定
NEC_FILE_PROTECTION	NFP を有効に設定します。	#1 ＊[値のデータ]には#を入力しないでください。
NFP_SU_ENABLE	緊急保護解除機能を有効に設定します。	#1 ＊[値のデータ]には#を入力しないでください。
NFP_SU_KEY	「3.6.2 NFP の緊急保護解除用の公開鍵の取得」で取得した NFP の緊急保護解除用の公開鍵を設定します。	欄外参照

NFP_SU_KEY の設定例

＊サンプルです。値には実際に取得したものを設定してください

<RSAKeyValue><Modulus>rTaBBbKqsUIncMAKwhmGBiK/c8/5yfpZ0F4snrllMRZVNQf/Os
NyiGtQoMUr7WFHGgibPJ9u9K1+XpG+NcllORWJ2/bQiemdA0fKEtrjEMH0nu7MsqRWtU0
6gopb5BTCOUuGOodn1GyYMHgLAbTwMg3MzgHpfns5PyqxXJIZrEZBfyAlP5jyVuEJu/IxF
KW18vTCgTtb+x6zR2dPtQEZAua2koUwf4imZKv0PEOIfxAF3rW6I7Wm4c5cHt3oiGprFAS

DMPJPz1GS/8ulZ5fF2iukUYy16FYbObD1PeWcnFos9QkF4eqhlMWjW8Xfa99HtBbZVKuN
CCKBngQ4o7fTWw==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>

NFP 形式の保護を利用する場合の設定（緊急保護解除機能無効）

＊NFP の緊急保護解除機能を無効にしてのご利用は推奨しません

プロパティ名	内容	値の設定
NEC_FILE_PROTECTION	NFP を有効に設定します。	#1 ＊［値のデータ］には#を入力しないでください。
NFP_SU_ENABLE	緊急保護解除機能を無効に設定します。	#0 ＊［値のデータ］には#を入力しないでください。
NFP_SU_KEY	空欄のままとします。	

3.6.5 インストール

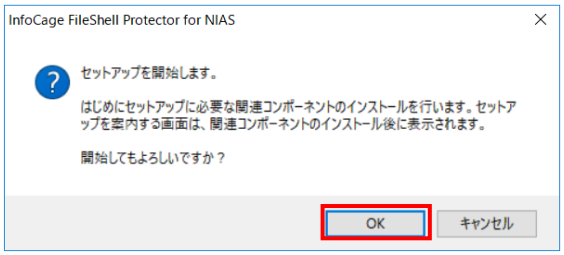
FileShell プロテクタ for NIAS をインストールする手順を説明します。

＊ 本ソフトウェアをインストールする際、InfoCage FileShell SDK も同時にインストールされます。

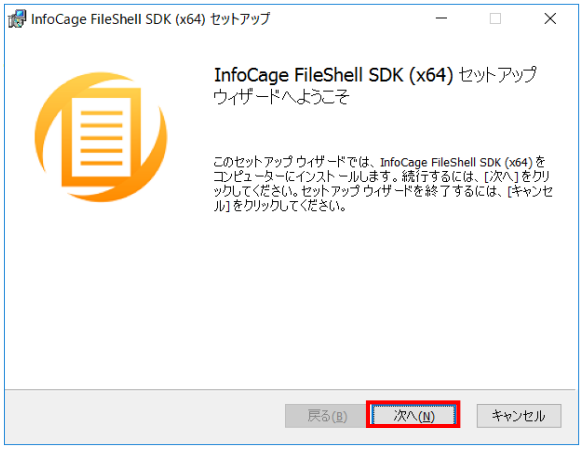
Operation

1. 展開したインストールパッケージの Setup フォルダー配下にある Setup.exe をダブルクリックしてください。

2. インストールの確認画面が表示されます。
[OK]をクリックしてください。

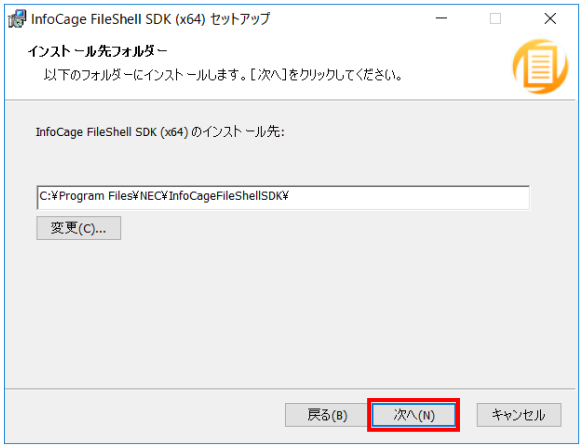


3. InfoCage FileShell SDK のインストールウィザードが表示されます。
[次へ]をクリックしてください。

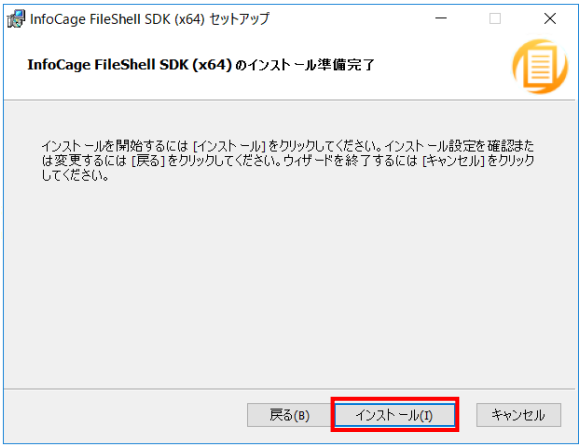


4. [インストール先のフォルダー]画面が表示されます。インストールフォルダーを指定し、[次へ]をクリックしてください。

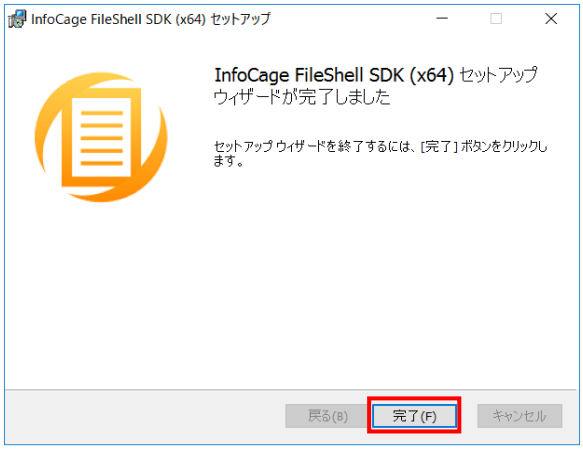
＊ InfoCage FileShell SDK は、デフォルトでは以下にインストールされます。
〈システムドライブ〉¥Program Files¥NEC¥InfoCageFileShellSDK¥



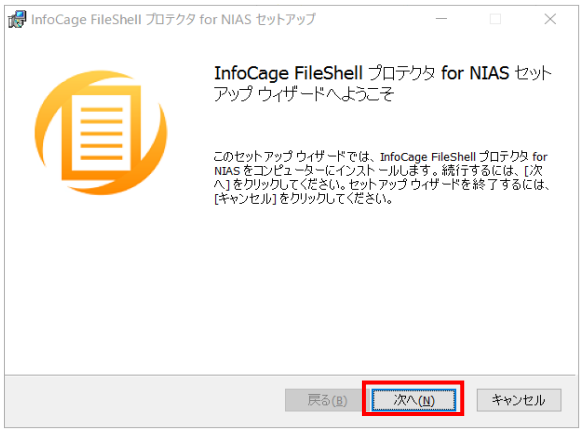
5. [インストール]をクリックし、インストールを実行してください。



6. FileShell SDK のインストールが完了すると、以下の画面が表示されます。[完了]をクリックしてください。

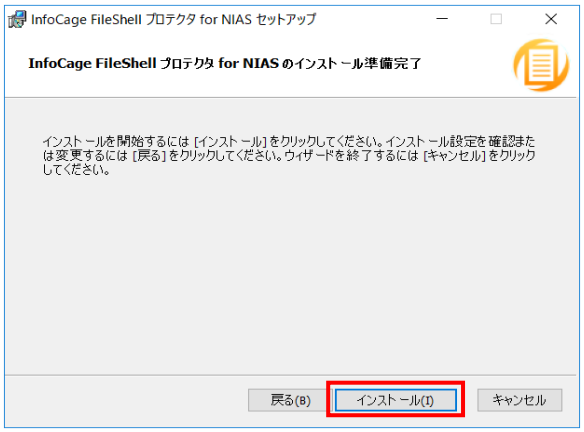


7. 続けて、FileShell プロテクタ for NIAS のインストールウィザードが表示されます。[次へ]をクリックしてください。

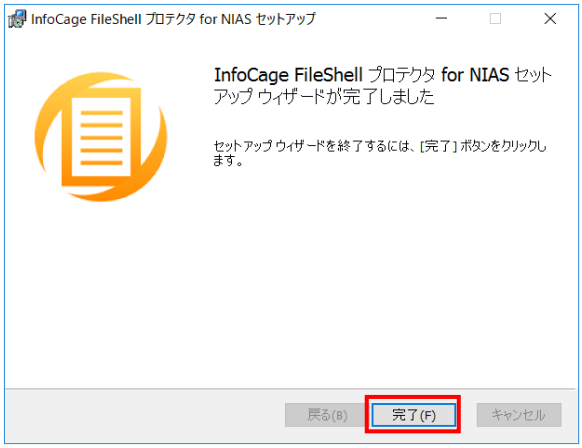


8. [インストール]をクリックし、インストールを実行してください。

＊ FileShell プロテクタ for NIAS は、手順 **4** で指定した、FileShell SDK のインストールフォルダーにインストールされます。



9. FileShell プロテクタ for NIAS のインストールが完了すると、以下の画面が表示されます。[完了]をクリックしてください。



以上で、FileShell プロテクタ for NIAS のインストールは、終了です。

3.6.6 バージョンアップインストール

FileShell プロテクタ for NIAS をバージョンアップインストールする場合は、インストーラーを実行し、バージョンアップをおこなってください。

参照 バージョンアップ方法は、インストール方法と同様です。「3.6.5 インストール」を参照してください。

3.7 RMS サーバーの接続設定

本ソフトウェアを使用して OfficeIRM 形式／FileShell 形式でファイルを保護をするためには、RMS のライセンスサーバーおよび認証サーバーの URL を環境設定ツールにて設定する必要があります。

＊ NFP 形式のみを使用する場合はこの設定は必要ありません。

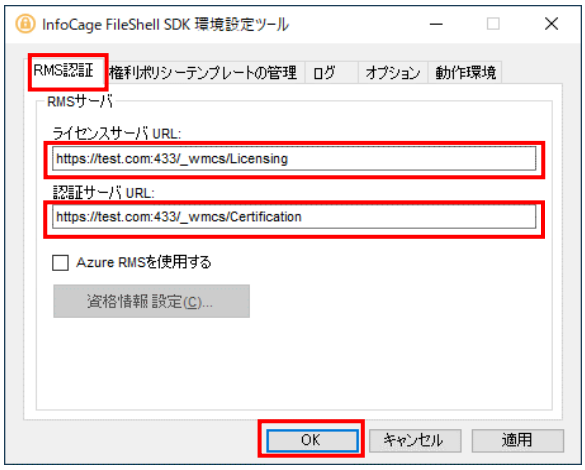
＊ OfficeIRM 形式／FileShell 形式で保護をするには RMS Client V2.1 がインストールされている必要があります。動作に必要なソフトウェアについては「1.3 動作環境について」および「3.2 必要なソフトウェアのインストール」を参照してください。

Operation

1. FileShell SDK インストール先の FileShellSDKSetting.exe を実行します。

   ＊ FileShell プロテクタ for NIAS は、デフォルトでは以下にインストールされます。
   <システムドライブ>¥Program Files¥NEC¥InfoCageFileShellSDK¥

2. [RMS 認証]タブを選択し、RMS サーバーの「ライセンスサーバ URL」および「認証サーバ URL」にそれぞれの設定内容を入力後、[OK]をクリックします。



   ＊ [RMS 認証]タブでの詳細な設定については「4.3.1 RMS 認証情報設定」を参照してください。

3.8 権利ポリシーテンプレートのインポート

本ソフトウェアを使用してファイルを保護するためには、保護時に使用する権利ポリシーテンプレート(xml 形式)をサーバーマシンにインポートする必要があります。

＊ MIP による分類/保護を利用する場合は本節の手順は不要です。

＊ 下記説明文中の<SID>には、本ソフトウェアを動作させる時に使用するアカウントのものが入ります。
SID は、本ソフトウェアを動作させる時に使用するアカウントでログオンし、コマンドプロンプトから、「whoami /user」コマンドを実行します。
コマンドの詳細については、「whoami /?」を実行してください。

3.8.1 Office IRM/FileShell 形式で保護する場合

Office IRM/FileShell 形式での保護を利用する場合は、アプリケーションの設計に従い、以下の手順で保護時に利用する RMS の権利ポリシーテンプレートをインポートします。

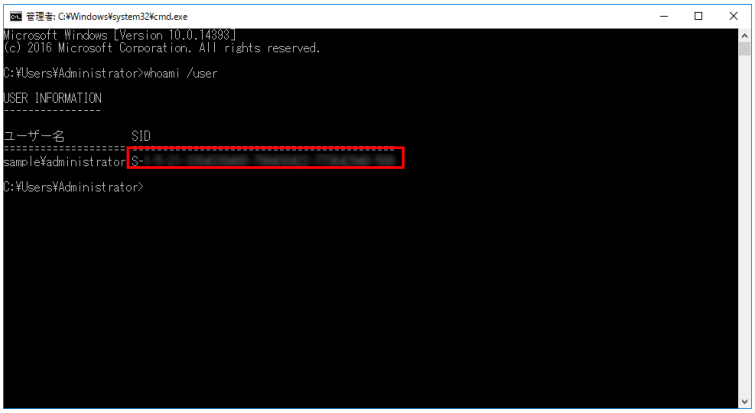
＊ Azure RMS サーバーで作成した権利ポリシーテンプレートを Unmanaged フォルダーに配置する場合、FileShell クライアントにて取得し、エクスポートしたものをご使用ください。
「3.5.2 Azure RMS サーバー上の権利ポリシーテンプレートの取得と保存」にて、PowerShell を用いて取得したものは使用できません。

＊「SYSTEM」、「LOCAL SERVICE」など、Windows のサービスアカウントで動作させる場合、手順 *2* で「FileShell SDK 環境設定ツール」を起動したあと、手順 *5* から実施してください。

Operation

1. 本ソフトウェアを動作させる時に使用するアカウントでログオンし、コマンドプロンプトから、「whoami /user」コマンドを実行し、SID(セキュリティ識別子)を確認します。

SID は手順 *4* で使用します。



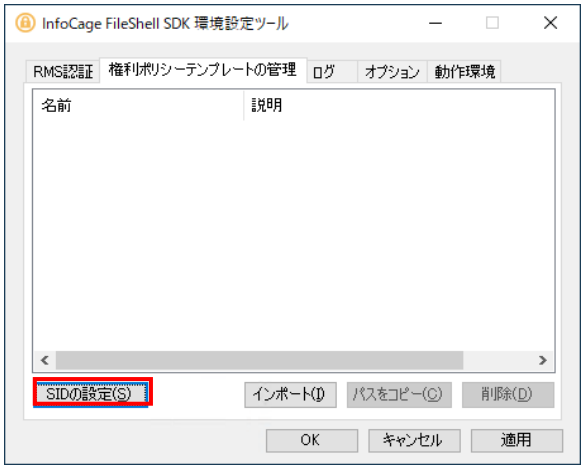
＊ SID は「S-」から始まるすべての文字列です。

＊ コマンドの詳細については、「whoami /?」を実行してください

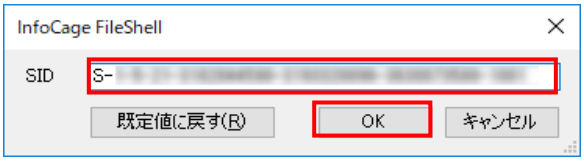
2. FileShell SDK インストール先の FileShellSDKSetting.exe を実行します。

＊ FileShell プロテクタ for NIAS は、デフォルトでは以下にインストールされます。
<システムドライブ>¥Program Files¥NEC¥InfoCageFileShellSDK¥

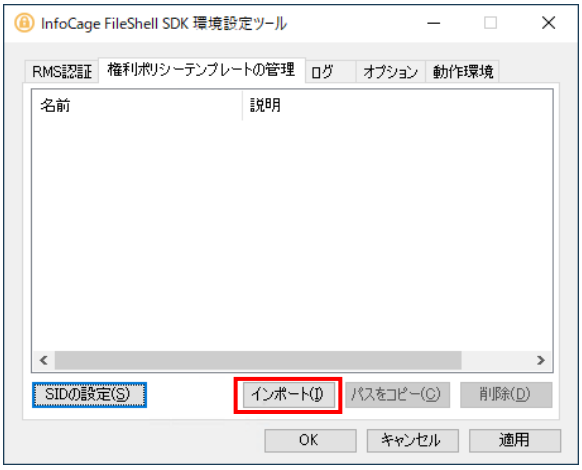
3. [権利ポリシーの管理]のタブを選択し、[SID の設定]を選択します。



4. SID の設定画面が表示されます。手順 *1* で確認した SID を[SID]に入力し、OK をクリックします。



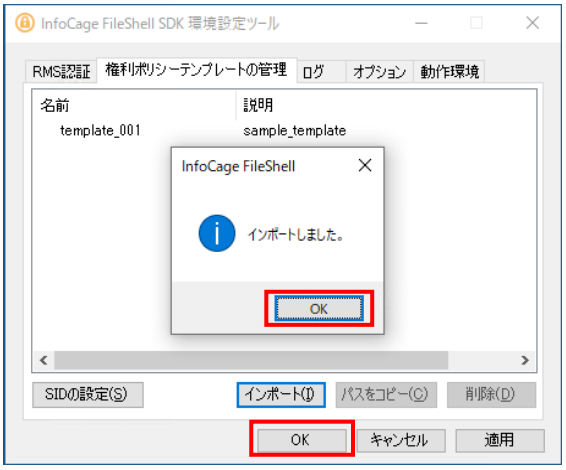
5. [権利ポリシーの管理]のタブを選択し、[インポート]を選択します。



6. 任意のフォルダーに格納した権利ポリシーテンプレート(xml 形式)を選択し、インポートします。

＊ Office IRM/FileShell 形式の保護を使用する場合、権利ポリシーテンプレートは保護機能を使用するユーザーごとに SID を設定して、インポートする必要があります。SID を変更した場合は、権利ポリシーテンプレートをインポートしなおしてください。

7. インポートが完了するとメッセージが表示され、一覧に権利ポリシーが追加されます。メッセージの OK ボタンクリックした後、下部の OK ボタンで環境設定ツールを閉じます。



以上で、Office IRM/FileShell 形式で保護する場合の権利ポリシーテンプレートのインポートは終了です。

3.8.2 NFP 形式で保護する場合

本ソフトウェアを使用してファイルを NFP 形式で保護するには、NFP 権利ポリシーテンプレート(xml 形式)を、SDK 環境設定ツール にてインポートする必要があります。

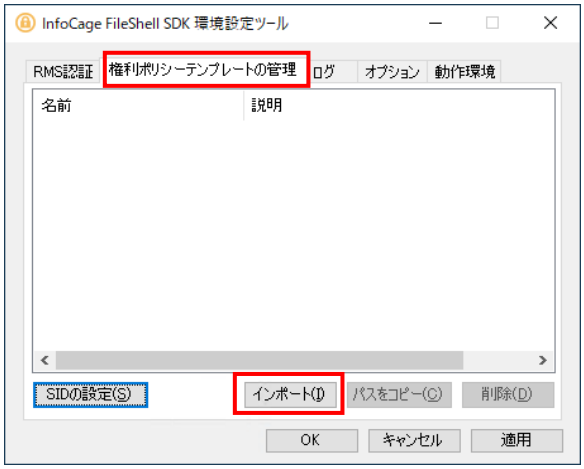
＊ 本ソフトウェアでは、パスワード暗号でエクスポート、もしくはバックアップされた NFP 権利ポリシーテンプレートを使用します。公開鍵暗号でエクスポートした NFP 権利ポリシーテンプレートはインポートできません。

Operation

1. FileShell SDK インストール先の FileShellSDKSetting.exe を実行します。

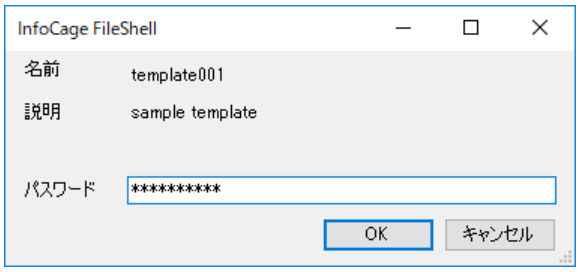
＊ FileShell プロテクタ for NIAS は、デフォルトでは以下にインストールされます。
〈システムドライブ〉¥Program Files¥NEC¥InfoCageFileShellSDK¥

2. [権利ポリシーテンプレートの管理]のタブを選択し、[インポート]を選択します。

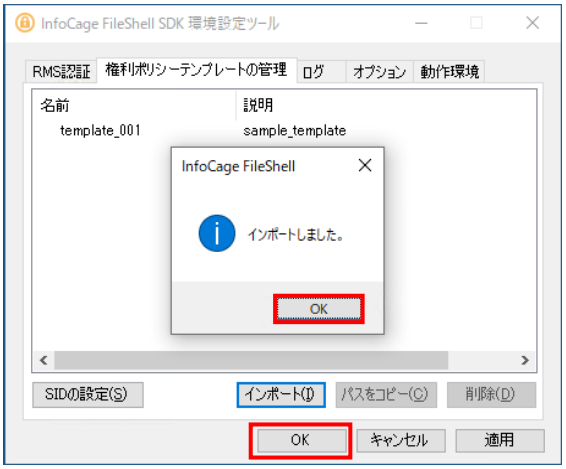


3. 任意のフォルダーに格納した NFP 権利ポリシーテンプレート(xml 形式)を選択し、インポートします。

＊ NFP 権利ポリシーテンプレート(xml 形式)をインポートするには、エクスポート時に設定されたパスワードによる認証が必要です。パスワードについては NFP 権利ポリシーの管理者に確認してください。



4. インポートが完了すると、メッセージが表示され、一覧に権利ポリシーが追加されます。メッセージの OK ボタンクリックした後、下部の OK ボタンで環境設定ツールを閉じます。



＊ 権利ポリシーのインポート完了後に環境設定ツールの[OK]／[適用]ボタンを押下した際に、サーバーURL が不正である旨のエラーメッセージが表示された場合は、[キャンセル]ボタン、もしくは右上の「×」ボタンで環境設定ツールを終了してください(同エラーメッセージが表示されても、本操作による権利ポリシーの追加は完了しています)。

以上で、NFP 形式で保護する場合の権利ポリシーテンプレートのインポートは終了です。

3.9 ラベル ID の取得

FileShell SDK でラベルを使用する際に指定するラベル ID(Guid)を取得します。

＊本項の手順を実行するには、Exchange Online PowerShell モジュールがインストールされている必要があります。インストールについては、『インストールガイド』の「MIP の利用に必要なモジュールのインストール」を参照してください。

Operation

1. Windows PowerShell から、本操作に必要となるモジュールをインストールします。
Windows の[スタートメニュー]からプログラムの一覧を表示し、[Windows PowerShell]の右クリックメニューから、「管理者として実行」を選択します。

2. 以下のコマンドを実行し、TLS1.2 を有効にします。

> [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bOR [Net.SecurityProtocolType]::Tls12

お使いの環境が Windows Server 2019 以降の場合は、本コマンドの実行は不要です。

3. 以下のコマンドを実行し、次のモジュールをインストールします。

- Exchange Online PowerShell モジュール

  > Install-module -Name ExchangeOnlineManagement

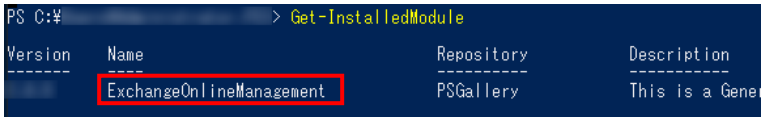
＊パッケージマネージャー「nuget」のインストール確認メッセージが表示された場合は、「Y」を入力して続行してください。

＊モジュールのインストール時に、「信頼されていないリポジトリからモジュールをインストールしようとしています。..」と表示された場合は、「Y」を入力して続行してください。

4. 以下のコマンドを実行し、モジュール一覧を取得します。

> Get-InstalledModule

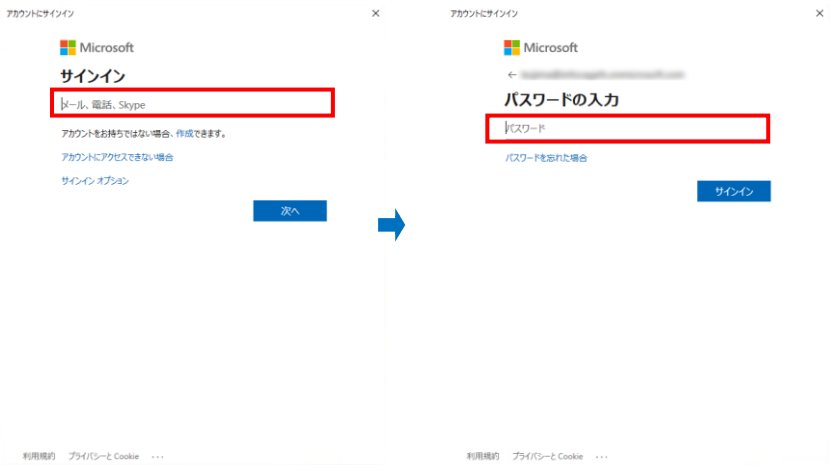
5. 一覧の「Name」に手順 *3* でインストールしたモジュールが表示されていることを確認します。



6. 以下のコマンドを実行します。

> Connect-IPPSSession

7. Microsoft のサインイン画面が表示された場合は、ユーザーID とパスワードを入力します。

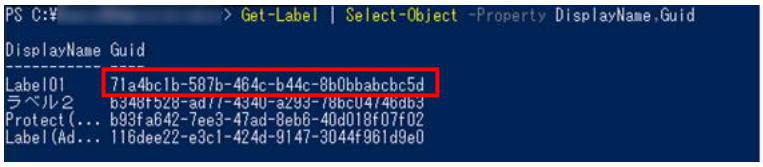


＊グローバル管理者の資格情報を持つユーザーで接続してください。

8. 以下のコマンドを実行します。

> Get-Label | Select-Object -Property DisplayName,Guid

9. ラベルの DisplayName と Guid が表示されますので、使用するラベルの Guid を控えます。



10. 以下のコマンドを実行して、接続を切断します。

Disconnect-ExchangeOnline

処理を続行してよいかを確認するメッセージが表示された場合は、「Y」を入力します。

以上で、ラベル ID の取得は終了です。

第4章 環境設定ツール

FileShellプロテクタ for NIASで、RMS認証や権利ポリシー、およびログなどの設定をおこなうには、環境設定ツールを使用します。本章では、それらの設定をおこなうための方法を記載します。

4.1 機能一覧

環境設定ツールでは、以下の機能を提供します。

機能名	概要
RMS 認証情報設定	RMS サーバーの認証に必要な情報を設定します。
権利ポリシー設定	権利ポリシーテンプレートをインポートし、使用する権利ポリシーのパスを取得します。
ログ出力情報設定	ログファイル出力に必要な情報を設定します。
オプション設定	動作に関する、その他の設定をおこないます。
動作環境表示	FileShell SDK のモジュール情報を表示します。

4.2 起動方法

FileShell プロテクタ for NIAS インストール時にインストールされる FileShell SDK インストール先の FileShellSDKSetting.exe を実行します。

＊ FileShell SDK は、デフォルトでは以下にインストールされます。

〈システムドライブ〉¥Program Files¥NEC¥InfoCageFileShellSDK¥

4.3 環境設定ツールの操作

環境設定ツールの操作について説明します。

4.3.1 RMS 認証情報設定

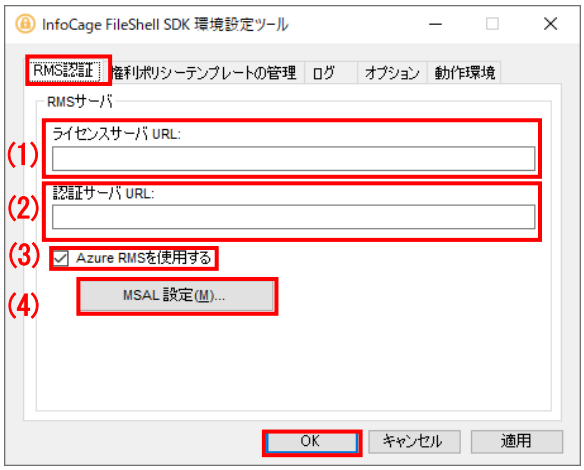
RMS の認証情報の設定は、FileShell プロテクタ for NIAS インストール時に初期設定をする場合、あるいは、RMS サーバー情報を変更する場合におこないます。

＊ NFP 形式のみを使用する場合は、この設定は必要ありません。

＊ NFP 形式のみを使用する場合は、FileShell での保護に RMS Client V2.1 は不要です。他の用途で必要なければアンインストールされることを推奨します。

Operation

1. ［RMS 認証］画面の各項目を指定して、［OK］をクリックします。



項目		内容
(1)	ライセンスサーバ URL	オンプレミスの RMS サーバーを利用する場合は、RMS ライセンスサーバーの URL を指定します。 例）https://test.com/_wmcs/licensing Azure RMS を利用する場合は、「3.4.4 Azure RMS のライセンスサーバー、および認証サーバーURL の取得」で取得した"LicensingIntranetDistributionPointUrl"を指定します。 例） https://aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee.rms.ap.aadrm.com/_wmcs/licensing ＊ MIP を利用する場合は設定不要です。 ＊ NFP のみを利用する場合は設定不要です。
(2)	認証サーバ URL	オンプレミスの RMS サーバーを利用する場合は、RMS 認証（証明）サーバーの URL を指定します。 例）https://test.com/_wmcs/certification Azure RMS を利用する場合は「3.4.4 Azure RMS のライセンスサーバー、および認証サーバーURL の取得」で取得した"CertificationIntranetDistributionPointUrl"を指定します。 例） https://aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee.rms.ap.aadrm.com/_wmcs/certification ＊ MIP を利用する場合は設定不要です。 ＊ NFP のみを利用する場合は設定不要です。
(3)	［Azure RMS を使用する］チェックボックス	MIP、もしくは Azure RMS を使用する場合にチェックします。 チェックボックスを ON にすると［MSAL 設定］ボタンが有効になります。
(4)	［MSAL 設定］ボタン	［MSAL 設定］画面を表示します。

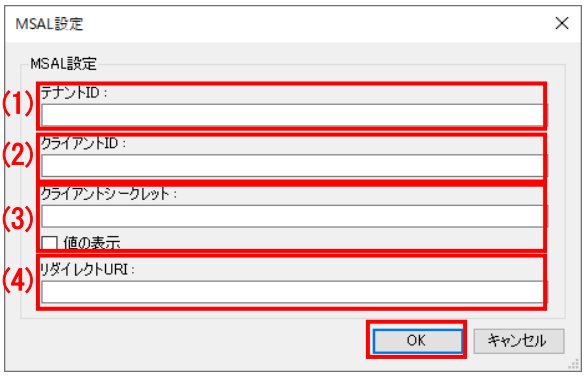
＊ ポート番号を含め、RMS サーバーの管理画面で表示されているのと同じ URL を指定してください。

＊ Azure RMS に接続するためにプロキシサーバーの設定が必要なネットワーク環境の場合、FileShell プロテクタ for NIAS を実行するアカウントにプロキシサーバーの設定が適用されている必要があります。各ユーザーのインターネットオプションから、設定をおこなってください。

2. MIP、もしくはAzure RMSを使用する場合は、[MSAL 設定]画面の各項目を指定して、[OK]をクリックします。

Notice

MSAL 設定で必要となる、クライアントシークレットは、有効期限が切れた場合、Azure RMS の認証がおこなえなくなるため、運用年数、セキュリティリスクなどを考慮の上、適切な期限を設定し、運用中に期限が切れることのないよう管理をおこなってください。
有効期限が切れた場合は、「3.4.3 クライアントシークレットの作成」に記載の手順でクライアントシークレットを再作成し、適用しなおしてください。

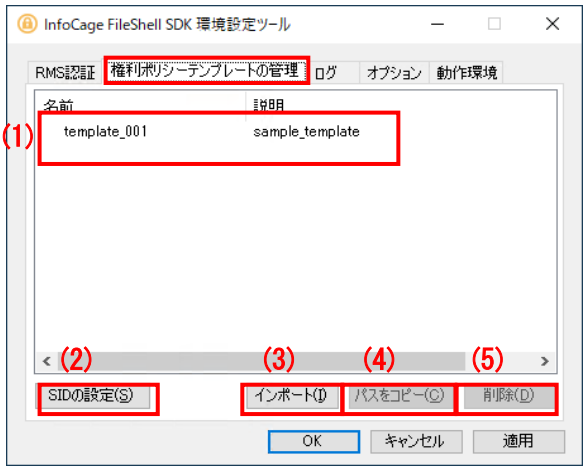


項目		内容
(1)	テナント ID	「3.4.1 Azure Portal でのアプリケーションの登録」で取得した「ディレクトリ(テナント)ID」を指定します。
(2)	クライアント ID	「3.4.1 Azure Portal でのアプリケーションの登録」で設定した「アプリケーション(クライアント)ID」を指定します。
(3)	クライアントシークレット	「3.4.3クライアントシークレットの作成」で作成したクライアントシークレットの値を指定します。 入力した値を確認したい場合は、[値の表示]にチェックを入れます。 ＊ プロテクタ for NIAS で使用する FileShell SDK は、V6.1 より Azure RMS を利用して保護/保護解除をおこなう場合の対称鍵(Symmetric Key) による認証はできなくなりました。 V6.1 未満のプロテクタ for NIAS からアップデートする場合など、従来の環境から引き続き Azure RMS を使用する場合でも、「3.4 MIP/Azure RMS を利用する場合に必要な情報の設定と取得」に記載の手順で Azure Portal にてアプリケーション登録～クライアントシークレット作成をおこない、クライアントシークレットの値を指定してください。
(4)	リダイレクト URI	「3.4.1 Azure Portal でのアプリケーションの登録」で設定したリダイレクト URI を指定します。

4.3.2 権利ポリシーテンプレートの管理

権利ポリシーテンプレートの管理は、利用する権利ポリシーテンプレートのインポートや削除などの管理をする場合におこないます。

Operation

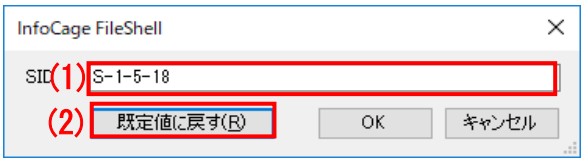


項目		内容
(1)	権利ポリシーテンプレートの一覧	現在選択されている SID にインポートされている権利ポリシーテンプレートを表示します。
(2)	SID の設定	権利ポリシーテンプレートを使用するアカウントの SID を設定します。 ＊ NFP 形式のみを利用する場合は使用しません。 また、RMS Client V2.1 がインストールされていない環境では、このボタンは表示されません。 ＊ Office IRM/FileShell 形式の保護を使用する場合、権利ポリシーテンプレートは保護機能を使用するアカウントごとに SID を設定して、インポートする必要があります。SID を変更した場合は、権利ポリシーテンプレートをその SID に対してインポートしなおしてください。
(3)	インポート	権利ポリシーテンプレート(xml ファイル)を選択し、FileShell プロテクタ for NIAS で権利ポリシーを使用可能にします。 ＊ SID が既定値以外の場合は、インポート前に SID の変更をおこなってください。
(4)	パスをコピー	権利ポリシーテンプレートのインポートパスを取得します。 ＊ ここで取得するパスは、「5.3 FileShell プロテクタ for NIAS の呼び出し設定」の手順 ***4.*** で、パラメーター名「ExtProgramArg_1」に指定するパスです。 ＊ 取得したパスはクリップボードにコピーされます。コピーされた内容や、メッセージは表示されません
(5)	削除	不要となった権利ポリシーを削除します。

4.3.2.1 SID の設定

権利ポリシーテンプレートを使用するプロセスの実行アカウントの SID を設定します。

＊SID は既定では LocalSystem(S-1-5-18)となっています。使用するアカウントに応じて SID を設定してください



項目		内容
(1)	SID	権利ポリシーテンプレートに関連づける SID を指定します。 適用するには、本欄に入力後、OK をクリックします。
(2)	既定値に戻す	SID を既定値に戻します。 ＊ 既定値は S-1-5-18(LocalSystem)です。

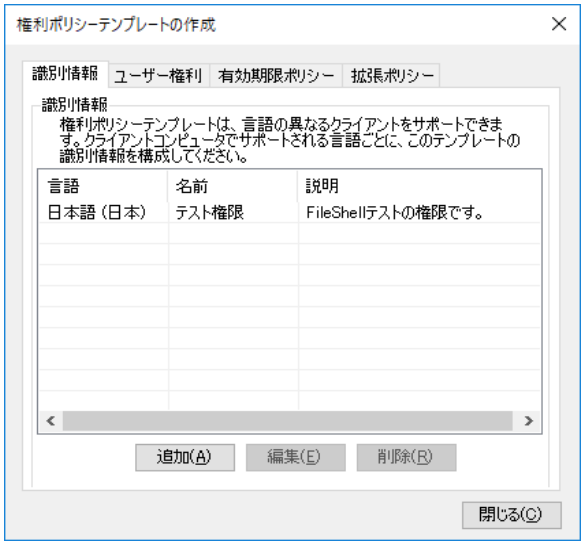
4.3.2.2 インポートされている権利ポリシーテンプレートの確認

権利ポリシーの一覧に表示されている権利ポリシーテンプレートをダブルクリックすることで、インポートされている権利ポリシーテンプレートの内容を確認します。

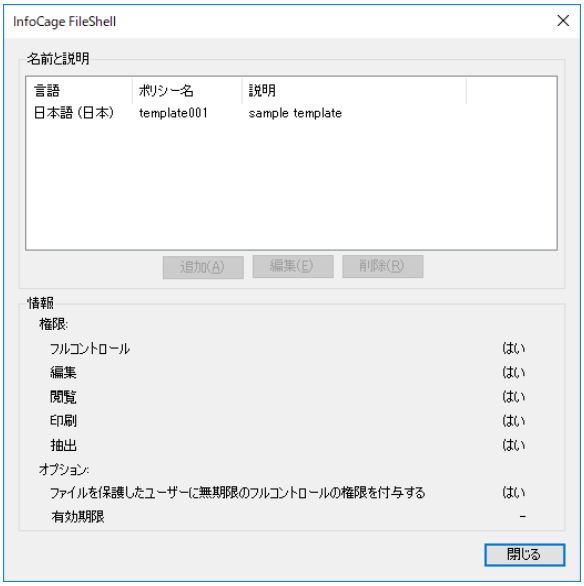
表示される内容は、RMS の権利ポリシーテンプレート、NFP 権利ポリシーテンプレートでそれぞれ異なります。

環境設定ツールでは、権利ポリシーテンプレートの内容を編集することはできません。
編集、削除等の操作をおこなっても、内容は保存されません

● **RMS の権利ポリシーテンプレートの場合**



● NFP 権利ポリシーテンプレートの場合



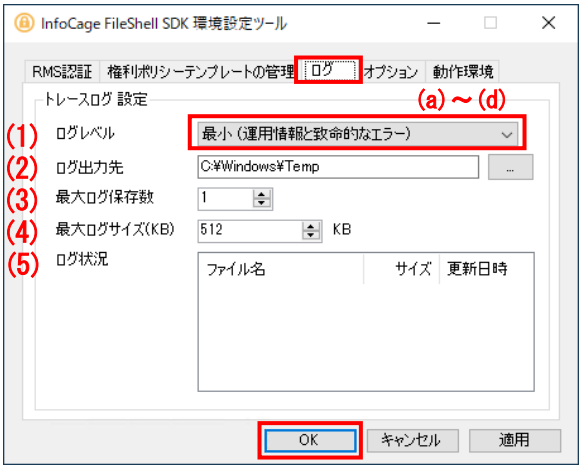
4.3.3 ログ出力情報設定

ログ出力情報の設定は、運用のためのログ設定をおこなう場合や FileShell プロテクタ for NIAS で何らかの問題が発生した場合など、ログレベルやサイズを変更したい場合におこないます。

本設定により出力されるログは、FileShell プロテクタ for NIAS で障害が発生した場合などに、製品サポート側での解析で利用します。

Operation

[ログ]の各項目を指定して、[OK]をクリックします。



項目		内容
(1)	ログレベル	ログのレベルを指定します。指定できるレベルは以下のとおりです。 (a)最小(運用情報と致命的なエラー) ・・・運用情報と致命的なエラーを出力します (b)中(一般エラー) ・・・(a)に加えて継続可能なエラーを出力します (c)大(警告) ・・・(b)に加えて重要な動作情報を出力します (d)詳細(デバッグ情報) ・・・(c)に加えて詳細な動作情報を出力します 既定値: (a)最小(運用情報と致命的なエラー)
(2)	ログ出力先	[参照]ボタンを選択し[フォルダーの参照]ダイアログよりログの出力先のディレクトリを選択します。本フォルダーへのアクセス権限は、FileShell SDK の実行アカウントに対し変更権限以上が必要です。 既定値:Windows ディレクトリの Temp
(3)	最大ログ保存数	最大ログサイズを超えた場合に、ローテートするログファイルの最大個数を指定します。(1～20) 既定値:1
(4)	最大ログサイズ(KB)	1 つのログファイルの最大サイズを KB 単位で指定します。(512～2,097,151(512K～2G)) 既定値:512
(5)	ログ状況	ログの出力先フォルダーに出力されているログファイルの情報を表示します。表示される情報は、ファイル名、サイズ、更新日時です。

4.3.4 オプション設定

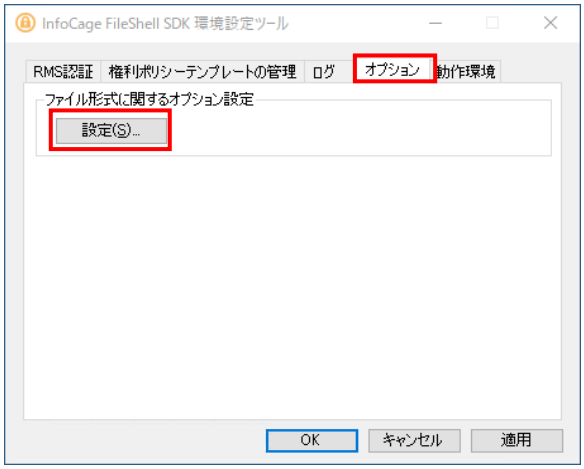
動作に関する、その他の設定をおこないます。

4.3.4.1 ファイル形式に関するオプション設定

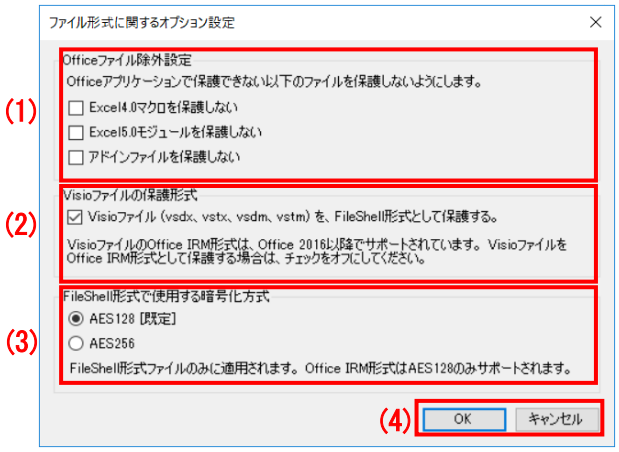
Office ファイルの除外設定および FileShell 形式の保護における暗号化方式の設定をおこないます。

＊ NFP 形式のみを使用する場合は、この設定は必要ありません。

[ファイル形式に関するオプション設定]の「設定」をクリックしてください。



「ファイル形式に関するオプション設定」画面



項目		内容
(1)	Office ファイル除外設定	
	[Excel4.0 マクロを保護しない]チェックボックス	Office アプリケーションで保護できない形式のファイルを、FileShell でも保護しないようにする場合に設定します。 ＊ 保護しないように指定した場合でも、以下の形式のファイルは保護されます。 ・ 読み取りパスワード付き Excel2007 形式 Excel アドインファイル
	[Excel5.0 モジュールを保護しない] チェックボックス	
	[アドインファイルを保護しない] チェックボックス	

(2)	Visio ファイルの保護形式	
	[Visio ファイル(vsdx、vstx、vsdm、vstm)を FileShell 形式として保護する]チェックボックス	Microsoft Visio のファイル(vsdx、vstx、vsdm、vstm)の保護に FileShell 形式を使用する場合にチェックを入れます。 ＊ チェックを外すと、Visio ファイルの保護に Office IRM 形式を使用します。 ＊ 既定は、チェック入(Visio ファイルを FileShell 形式として保護する」です。
(3)	FileShell 形式で使用する暗号化方式	
	[AES128]ラジオボタン	FileShell 形式での保護(暗号化)に、AES128 を使用します(既定)。
	[AES256]ラジオボタン	FileShell 形式での保護(暗号化)に、AES256 を使用します。
(4)	[OK]ボタン	ファイル形式に関するオプションを設定し「オプション設定」画面に戻ります。
	[キャンセル]ボタン	キャンセルします。

＊「FileShell 形式で使用する暗号化方式」の設定が AES256 を使用する設定の場合でも、OfficeIRM 形式では、AES128 で保護(暗号化)されます。

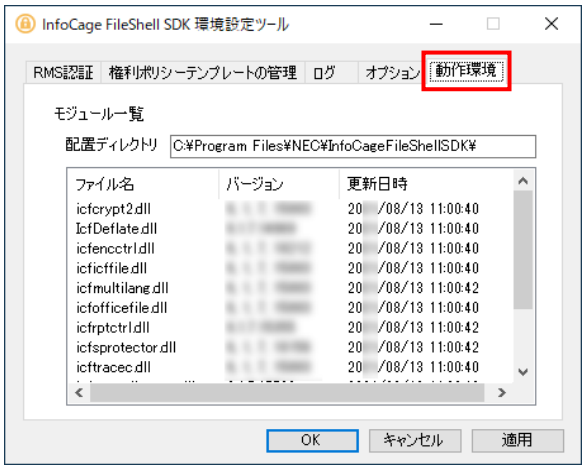
＊「FileShell 形式で使用する暗号化方式」の設定により、AES256 を使用して保護されたファイルは、FileShell クライアント Ver.3.0 以前の環境で開くことはできますが、保存することはできません。(ただし、Ver.3.0.291.9561 以降は、保存も可能となります。)
なお、FileShell クライアント Ver.3.1 以降では、保護されたファイルが AES128、AES256 で混在している場合でも読み書きすることができます。

4.3.5 動作環境表示

FileShell プロテクタ for NIAS の動作環境情報を表示します。

動作環境情報の表示は、FileShell プロテクタ for NIAS が正常に動作しない場合など、FileShell プロテクタ for NIAS のモジュール情報を確認したい場合におこないます。

＊ 本画面では、モジュール情報の確認のみ可能です、この画面で設定の変更などをおこなうことはできません。



4.3.6 設定情報ファイル出力

環境設定ツールの[OK]ボタン、または、[適用]ボタンをクリックしたタイミングで、環境設定ツールで設定した情報やFileShell プロテクタ for NIASのモジュールバージョンの一覧が記載された設定情報ファイルが出力されます。

このファイルは障害が発生し、製品サポート側にFileShell プロテクタ for NIASの設定情報を送付しなければならない場合などに利用します。

《ファイル名》

IcfsProtector.env

《出力先》

ログ出力先フォルダー

《形式》

[Environment]

動作環境情報

[RMS Authenticate]

RMS 認証情報

[Log]

ログ出力設定情報

第5章 NIAS のインストール

FileShell プロテクタ for NIAS のインストール後、NIAS から FileShell プロテクタ for NIAS を呼び出すための手順を説明します。

5.1 NIAS 製品本体、エージェントのインストール

FileShell プロテクタ for NIAS をインストールした後、同サーバー上に NIAS Ver.4.1 以降のインストールが必要です。NIAS 製品本体、またはエージェントのインストールは NIAS の CD メディア内の Documents フォルダー配下にある製品マニュアル「セットアップガイド.pdf」をご参照ください。
ただし、以下の注意事項がありますので、あわせてご確認ください。

* NIAS インストール時に指定する NIAS のサービス実行ユーザーに、ローカルの管理者権限を持つドメインユーザーカウントを指定してください。
* サービス実行ユーザー(ドメインユーザーカウント)には電子メール アドレスが設定されている必要があります。
* NIAS エージェントのみインストールしたサーバーについても FileShell プロテクタ for NIAS のセットアップは必要になりますのでご注意ください。

5.2 保護(暗号化)メニューの画面表示設定

NIAS をインストール後、NIAS の「検索」画面や「個人情報」画面に、FileShell プロテクタ for NIAS を使用して保護(暗号化)をおこなう整理メニューを追加するために、プロパティファイルを修正します。

* NIAS エージェントのみインストールしたサーバーの場合、本手順は必要ありません。

5.2.1 プロパティファイル(日・英)を修正する

修正対象のプロパティファイルは日本語、英語それぞれ以下にあります。

C:¥Program Files¥Apache Software Foundation¥Tomcat 9.0¥webapps¥ias-manager¥WEB-INF
¥classes¥com¥nec¥jp¥ias¥gui¥common¥property¥

- MessageResource_ja.properties ← 日本語プロパティファイル
- MessageResource.properties ← 英語プロパティファイル

以下の手順では日本語プロパティファイルの修正手順を記載します。英語プロパティファイルも同様の手順で修正してください。

* 修正する際は上記 2 ファイルのバックアップを必ずとってください。
* プロパティファイルの修正には JDK が必要になります。Oracle 社 Web サイトから JDK8 をダウンロードし、事前にインストールしてください(JDK8 が入手できない場合は、NEC 保守窓口までお問合せください)。

Operation

1. コンピューターの管理者(Administrator)権限を持つアカウントで、NIAS をインストールした Windows サーバーにログインします。

2. 以下の手順で「Apache Tomcat」サービスを停止してください。

   ＊「スタートメニュー」 → 「管理ツール」 → 「サービス」 → 「Apache Tomcat 9.0 Tomcat9」を右クリック → 「停止」

3. 修正ファイルを日本語で読める形式に変換するため、コマンドプロンプトを以下の手順で起動してください。

   ＊「スタートメニュー」 → 「すべてのプログラム」 → 「アクセサリ」 → 「コマンド プロンプト」を右クリック → 「管理者として実行」

4. NIAS インストール時に自動的にインストールした Java の実行プログラム格納フォルダーに移動するため、コマンドプロンプトから以下の文を実行してください。

```
> cd "c:¥Program Files¥Java¥jdk1.8.0_201¥bin"
```

   ＊ 上記の移動コマンドの実行に失敗した場合は NIAS サーバーにインストールされている Java (JDK)のパスを確認した上で、上記コマンドのパス文字列を変更して実施してください。

5. 修正ファイルを読める形式に変換するため、コマンドプロンプトから以下の文を実行してください。

```
> native2ascii.exe -reverse "c:¥Program Files¥Apache Software Foundation¥Tomcat 9.0¥webapps¥ias-manager¥WEB-INF¥classes¥com¥nec¥jp¥ias¥gui¥common¥property¥MessageResource_ja.properties" "c:¥MessageResource_ja_tmp.properties"
```

   ＊ 上記コマンド例では、修正ファイル(MessageResource_ja.properties)を日本語で読める形式に変換したファイルを C ドライブ直下に"MessageResource_ja_tmp.properties"というファイル名で保存します。

6. 前手順で変換したファイルをメモ帳などの任意のテキストエディタで開いてください(前述の手順例では C ドライブ直下に"MessageResource_ja_tmp.properties"というファイル名で保存しています)。ファイルを開いた際に、2 バイト文字(日本語等)が読める形式となっていることを確認してください。

7. 以下のパラメーター名を探して、「=」で区切られた後ろの文字列を編集して保存してください。修正例を赤字で示します。

```
#整理メニューに表示される表示名を指定します
param.operation.method.command.label=保護(暗号化)
#整理メニューの表示に上記で設定した項目を追加するため末尾に command を追加します
order.operation.method=move,archive,boxmove,moveback,trashbox,delete,compress,copy,flagoff,necessary,unnecessary,owner,command
#個人情報整理の検出リスト画面に保護ボタンを表示する場合は true
personal.exec.command.display=true
#個人情報整理の検出リスト画面で保護(暗号化)実行時の確認メッセージ
message.personal.command.confirm=選択したファイルに対して保護(暗号化)を実行します。よろしいですか？
```

   ＊ 上記のコメント欄(#)はパラメーター名の説明です。実際のプロパティファイルに上記の説明はありませんのでご注意ください

＊ 元々の設定値をファイル内に残して無効化するため、元々の設定値の先頭に「#」を付けることを推奨します

8. 編集したファイルを本来のファイル名に上書き適用するため、コマンドプロンプトから以下の文を実行してください。

```
> native2ascii.exe "c:¥MessageResource_ja_tmp.properties" "c:¥Program Files¥Apache Software Foundation¥Tomcat 9.0¥webapps¥ias-manager¥WEB-INF¥classes¥com¥nec¥jp¥ias¥gui¥common¥property¥MessageResource_ja.properties"
```

9. 以下の手順で「Apache Tomcat」サービスを開始してください。

＊ 「スタートメニュー」 → 「管理ツール」 → 「サービス」 → 「Apache Tomcat 9.0 Tomcat9」を右クリック → 「開始」

10. 上記手順内で一時的に日本語化したファイル（手順例では c:¥MessageResource_ja_tmp.properties）は削除するなどしてください。

5.3 FileShell プロテクタ for NIAS の呼び出し設定

「5.2 保護(暗号化)メニューの画面表示設定」で設定した保護(暗号化)の整理メニューが選択された際に FileShell プロテクタ forNIAS が呼び出されるよう設定ファイルに連携設定をおこないます。修正対象の設定ファイルは以下にあります。

C:¥Program Files (x86)¥NEC¥NIAS¥Operation¥File¥config¥config.xml

＊ 上記は既定のインストール先の場合です。インストールフォルダーを変更している場合は読み替えてください。

Operation

1. 上記の設定ファイルをメモ帳等のテキストエディタで開きます。

＊ 環境により保存時に権限不足エラーが発生する可能性があります。その際は、エディタを管理者権限で起動してから上記該当の設定ファイルを開いてください。

2. パラメーター名「ExtProgramPath」を探し、設定値に FileShell プロテクタ for NIAS の実行ファイルパスを指定します。

```
#設定例
<property>
  <name>ExtProgramPath</name>
  <value>C:¥Program Files¥NEC¥InfoCageFileShellSDK¥IcfCryptFL.exe</value>
  <description>外部連携プログラムパス(フルパス指定)</description>
</property>
```

＊ FileShell プロテクタ for NIAS のインストールパスを変更している場合は読み替えてください。

3. パラメーター名「ExtProgramArg」を探し、設定値を指定します。

＊ Office IRM/FileShell 形式で保護をする場合と NFP 形式で保護をする場合で一部設定値が異なります。
（下記設定例 ◯ の個所）

● Office IRM/FileShell 形式で保護をする場合

設定値に「/target {0} /template {1} /encType 0 /repType 0」を指定します。

```
#設定例
<property>
  <name>ExtProgramArg</name>
  <value>/target {0} /template {1} /encType 0 /repType 0</value>
  <description>外部連携プログラムコマンド引数文字列</description>
</property>
```

● Microsoft 互換/FileShell(ラベル)形式で分類/保護をする場合

設定値に「/target {0} /template {1} /encType 6 /repType 0」を指定します。

```
#設定例
<property>
  <name>ExtProgramArg</name>
  <value>/target {0} /template {1} /encType 6 /repType 0</value>
  <description>外部連携プログラムコマンド引数文字列</description>
</property>
```

● NFP 形式で保護をする場合

設定値に「/target {0} /template {1} /encType 5 /repType 0」を指定します。

```
#設定例
<property>
  <name>ExtProgramArg</name>
  <value>/target {0} /template {1} /encType 5 /repType 0</value>
  <description>外部連携プログラムコマンド引数文字列</description>
</property>
```

＊ encType を使用せず、設定値を「/target {0} /template {1} /repType 0」とし、/template に指定する権利ポリシーテンプレート、またはラベル ID を使い分けることで、保護形式を指定することもできます。

● Office IRM/FileShell 形式で保護をする場合

設定値の/template に Office IRM/FileShell 形式の保護で使用する権利ポリシーテンプレートのパスを指定します。

● Microsoft 互換/FileShell(ラベル)形式で分類/保護をする場合

設定値の/template に Microsoft 互換/FileShell(ラベル)形式の分類/保護で使用するラベルのラベル ID を指定します。

● **NFP 形式で保護をする場合**

設定値の/template に NFP 形式の保護で使用する権利ポリシーテンプレートのパスを指定します。

＊ /template の詳細な設定例については、手順 *4* を参照してください。

＊ Office IRM/FileShell 形式、または NFP 形式で保護をする場合に使用する権利ポリシーテンプレートのパスは、以下の手順で取得し、指定します。

1. 「3.8 権利ポリシーテンプレートのインポート」で権利ポリシーテンプレート(xml ファイル)をインポートします。

2. 「4.3.2 権利ポリシーテンプレートの管理」タブを参照し、環境設定ツールの[パスをコピー]ボタンを押します。

3. 2 で取得したパスを指定します(指定方法の詳細は以下の 2 つのケースを参照ください)

＊ Microsoft 互換/FileShell(ラベル)形式で分類/保護をする場合に使用するラベル ID の取得方法については「3.9 ラベル ID の取得」を参照してください。

4. パラメーター名「ExtProgramArg_1」を探し、設定値に権利ポリシーテンプレートのパス、またはラベル ID を指定します。

Office IRM/FileShell 形式、または NFP 形式で保護をする場合は、以下の手順で権利ポリシーテンプレートのパスを取得し、指定します。

1. 「3.8 権利ポリシーテンプレートのインポート」で権利ポリシーテンプレート(xml ファイル)をインポートします。

2. 「4.3.2 権利ポリシーテンプレートの管理」タブを参照し、環境設定ツールの[パスをコピー]ボタンを押します。

3. 2 で取得したパスを指定します。

```
#設定例
<property>
  <name>ExtProgramArg_1</name>
  <value>
"C:¥ProgramData¥Microsoft¥MSIPC¥Server¥UnmanagedTemplates¥S-1-5-21-2993025969-137
0399536-2746055028-2736¥Policy.xml"</value>
```

＊上記設定値は実行ユーザーSID やテンプレートファイル名で変わってきますのでご注意ください。
＊上記設定値はダブルクォートで必ず囲んでください。

Microsoft 互換/FileShell 形式で分類/保護をする場合は、「3.9 ラベル ID の取得」で取得したラベル ID を指定します。

```
#設定例
<property>
  <name>ExtProgramArg_1</name>
  <value> "{71a4bc-857b-464c-b44c-8b0bbabcbc5dl}"</value>
  <description>外部連携プログラムパス(フルパス指定)</description>
</property>
```

＊ 「3.9 ラベル ID の取得」で取得したラベル ID を{ }付きで指定してください。
＊ 上記設定値は{ }を含め、ダブルクォートで必ず囲んでください。

5. 上書き保存して完了です。サービス再起動などは不要で即時反映されます。

5.4 保護(暗号化)の実行方法

NIAS の画面から FileShell プロテクタ for NIAS を呼び出し、対象ファイルを保護(暗号化)する手順を説明します。

＊ 本節での「保護(暗号化)」は、MIP のラベル付与による「分類」を含みます。

実施する画面は「検索」画面と「個人情報」画面の 2 つがあります。

＊ 後者は「個人情報検出オプション」も必要になりますのでご注意ください。

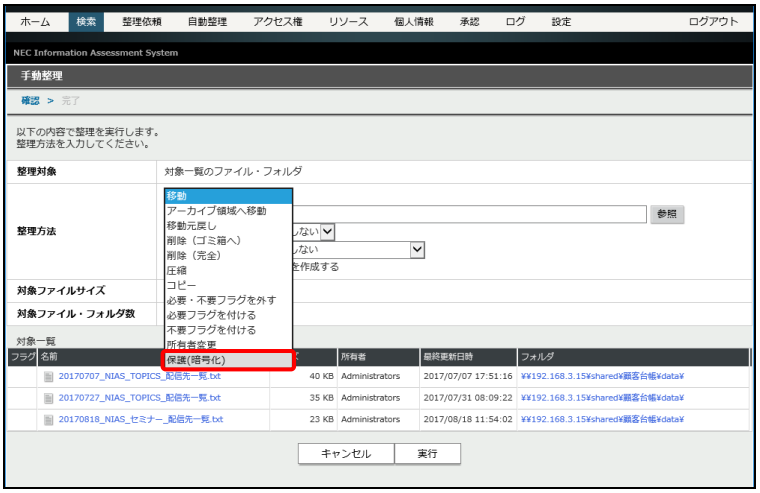
5.4.1 検索画面から保護(暗号化)する

「検索」画面から手動でファイルを保護(暗号化)する手順を説明します。なお、自動整理の機能で保護(暗号化)を自動的に実行することも可能です。詳細な手順は NIAS の CD メディア内の Documents フォルダー配下にある「ファイル整理ガイド」をご参照ください。

Operation

1. NIAS にログイン後、「検索」メニューを選択します。
2. フォルダーツリーから検索対象パスを選択して、「条件指定」で保護(暗号化)したいファイルの条件を指定して「検索」ボタンを押します。
3. リストから保護(暗号化)したいファイルにチェックを入れて、ページ最下部の「手動整理」を選択します。
4. 「整理方法」のプルダウンの「保護(暗号化)」を選択して「実行」を押します。

   ＊ 整理メニューの表示名を変更している場合は読み替えてください。



5. 非同期で実行されますので、実行結果は「ログ」メニューから確認してください。

5.4.2 個人情報画面から保護(暗号化)する

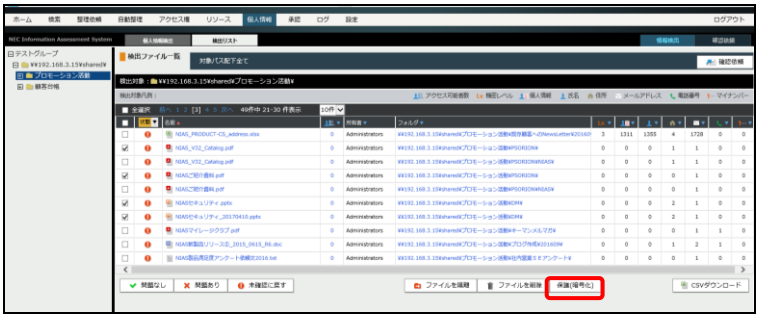
「個人情報」画面からファイルを保護(暗号化)する手順を説明します。

Operation

1. NIAS にログイン後、「個人情報」メニューを選択します。
2. フォルダーツリーから検出対象パスを選択して、「個人情報検出」タブの方で保護(暗号化)対象とする個人情報ファイルの条件を指定します。

   ＊ 条件の指定方法については NIAS の「個人情報検出オプションガイド」をご参照ください。

3. 対象を絞り込んだら「検出リスト」タブに遷移して、表示されているファイルリストの中から保護(暗号化)したいファイルにチェックを入れて、ページ最下部の「保護(暗号化)」を選択します。



   ＊ 整理メニューの表示名を変更している場合は読み替えてください。

4. 非同期で実行されますので、実行結果は「ログ」メニューから確認してください。

第6章 アンインストール

FileShell プロテクタ for NIAS をアンインストールする手順を説明します。NIAS のアンインストールについては NIAS の CD メディア内の Documents フォルダー配下にある「セットアップガイド.pdf」をご参照ください。

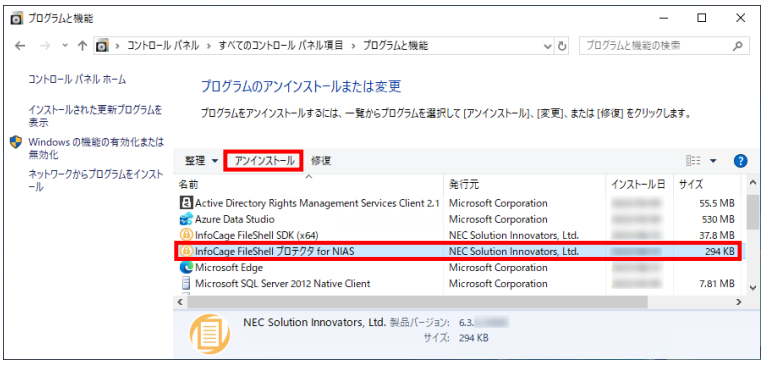
＊ FileShell プロテクタ for NIAS と NIAS の両方をアンインストールする場合、どちらからアンインストールをおこなっても問題ありません。

＊ FileShell プロテクタ for NIAS のみアンインストールして、NIAS はアンインストールしない場合は、「5.2 保護(暗号化)メニューの画面表示設定」で設定した内容を元に戻してください。

Operation

1. コンピューターの管理者(Administrator)権限を持つアカウントで、Windows のスタートメニューから、[コントロールパネル]-[プログラムと機能]を選択します。

2. インストールされているプログラムの一覧が表示されますので、[InfoCage FileShell プロテクタ for NIAS]を選択して、[アンインストール]をクリックします。



3. アンインストールの確認画面が表示されますので[はい]をクリックします。

4. インストールされているプログラムの一覧から、[InfoCage FileShell プロテクタ for NIAS]が削除されていることを確認します。

5. 続けて、InfoCage FileShell SDK をアンインストールします。
手順 2～4 を参考に、「InfoCage FileShell SDK(x64)」をアンインストールします。

6. インストールされているプログラムの一覧から、[InfoCage FileShell SDK(x64)]が削除されていることを確認します。

＊ InfoCage FileShell プロテクタ for NIAS、および InfoCage FileShell SDK をインストール後に OS の再起動をする必要はありません。

以上で、FileShell プロテクタ for NIAS のアンインストールは、終了です。

InfoCage FileShell Ver 6.3
FileShell プロテクタ for NIAS
利用ガイド

NEC ソリューションイノベータ株式会社

東京都江東区新木場一丁目 18 番 7 号
TEL(03)5534-2222 (代)

Copyright© NEC Solution Innovators, Ltd. 2021-2023.

NEC ソリューションイノベータ株式会社の許可なく複製・改変等を行うことはできません。