

kaspersky

# Kaspersky Security for Storage 製品紹介

2021年10月11日

株式会社カスペルスキー

セールスエンジニアリング部

# Kaspersky Security for Storage



## 各種NASへのリアルタイム保護

多くの受賞歴を誇るカスペルスキーのエンジン。  
プロアクティブなセキュリティを可能にする。



## RPC と ICAPに準拠したNASのサポート

エンタープライズ市場で多く使用されるNASを保護。  
高度な脅威から防御。



## 冗長性と負荷分散

冗長性を目的として複数の保護サーバーを構築可能。  
NAS間の負荷を均衡させる。



## ハイパフォーマンスと効率性

NASのパフォーマンスへの影響を抑えた、  
最適化されたテクノロジー。



## 柔軟でパワフルなレポート機能

セキュリティの観点から、データストレージインフラ  
ストラクチャー全体を可視化



## 除外と信頼

セキュリティスキャンから除外する「信頼ゾーン」を  
作成、細かな設定を施したスキャンパフォーマンス。



## アプリケーション起動コントロール

Windows Server上で、信頼されていない  
アプリケーション、実行ファイルを起動させない。



## ホストのブロック、アンチクリプター

Windows Server上の共有ファイルに対する危険な  
感染、ランサムウェアから保護。信頼出来ない  
ホストからのアクセスをブロック

\* Windows Serverのみ, NASに対しては動作しない

# サポートされるプラットフォームとプロトコル



- Isilon: OneFS
- Celerra/VNX:
- Unity など

ICAP

CAVA

CEE

OAS

ODS



Alliance Partner

- 7-mode
- Cluster-mode Data ONTAP
- ONTAP

RPC

OAS

ODS



Gold Partner

- Oracle ZFS Storage: all appliances

ICAP

OAS



- Hitachi HNAS: 3080, 3090, 4040, 4060, 4080, 4100

ICAP

RPC

OAS



- DELL FS8600: FluidFS 5.x

ICAP

OAS



- Acropolis File Services

ICAP

OAS



- HP 3PAR-Series

ICAP

OAS

ODS

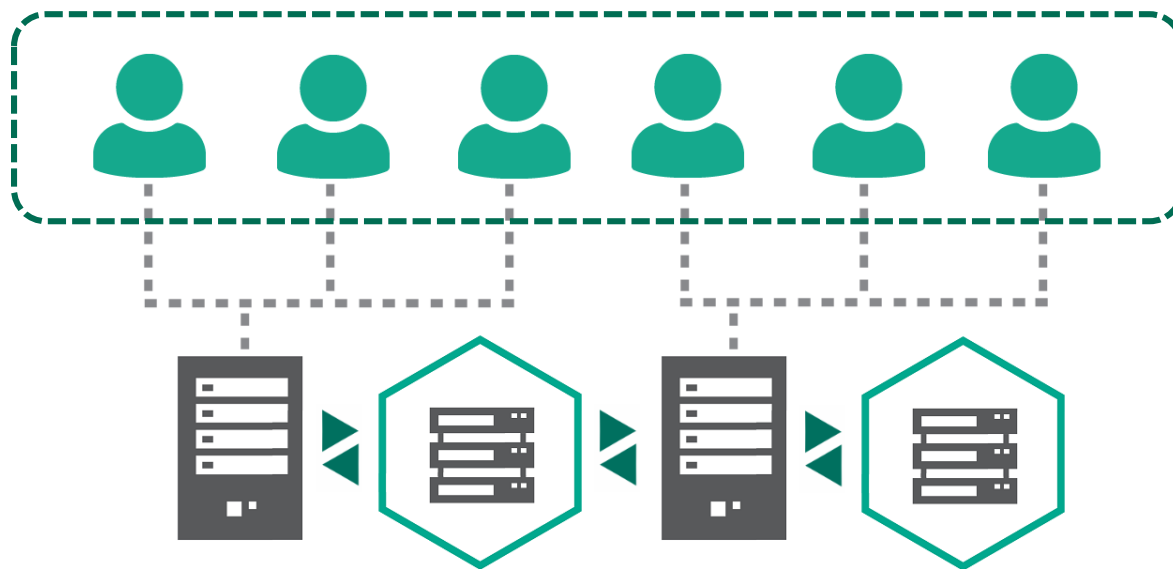
OAS オンアクセススキャン  
ODS オンデマンドスキャン

: P9へ

サポートNAS システム要件  
<https://support.kaspersky.com/KSWS/11.0.1/ja-jp/155511.htm>

# 製品ライセンス体系

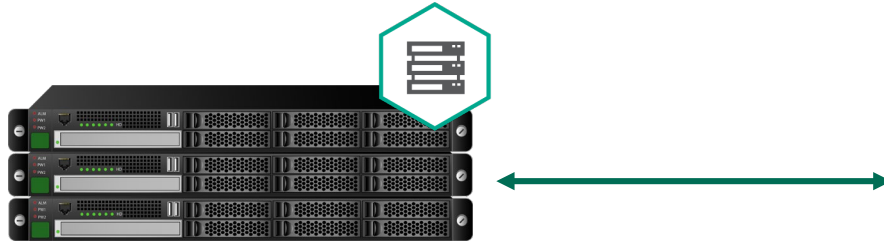
NASを使用するユーザー数（端末数） トータル数による課金



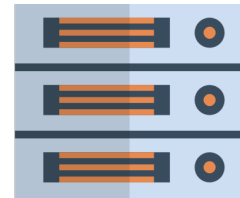
NASが複数台あり、Kaspersky Security for Storageが複数台あっても、使用するユーザー数（端末数） トータル数で計算すれば良い。

# Kaspersky Security for Storage基本構成

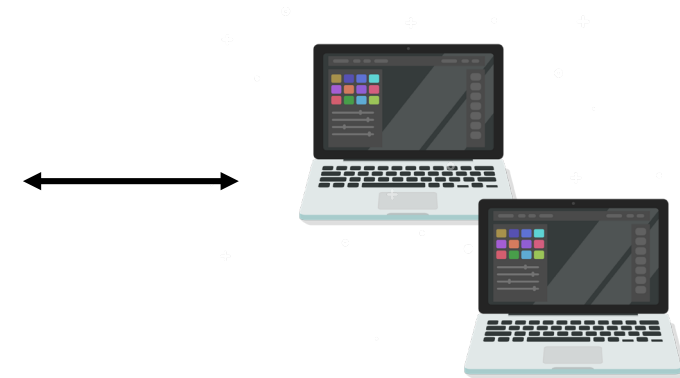
Kaspersky Security for Storage



NAS

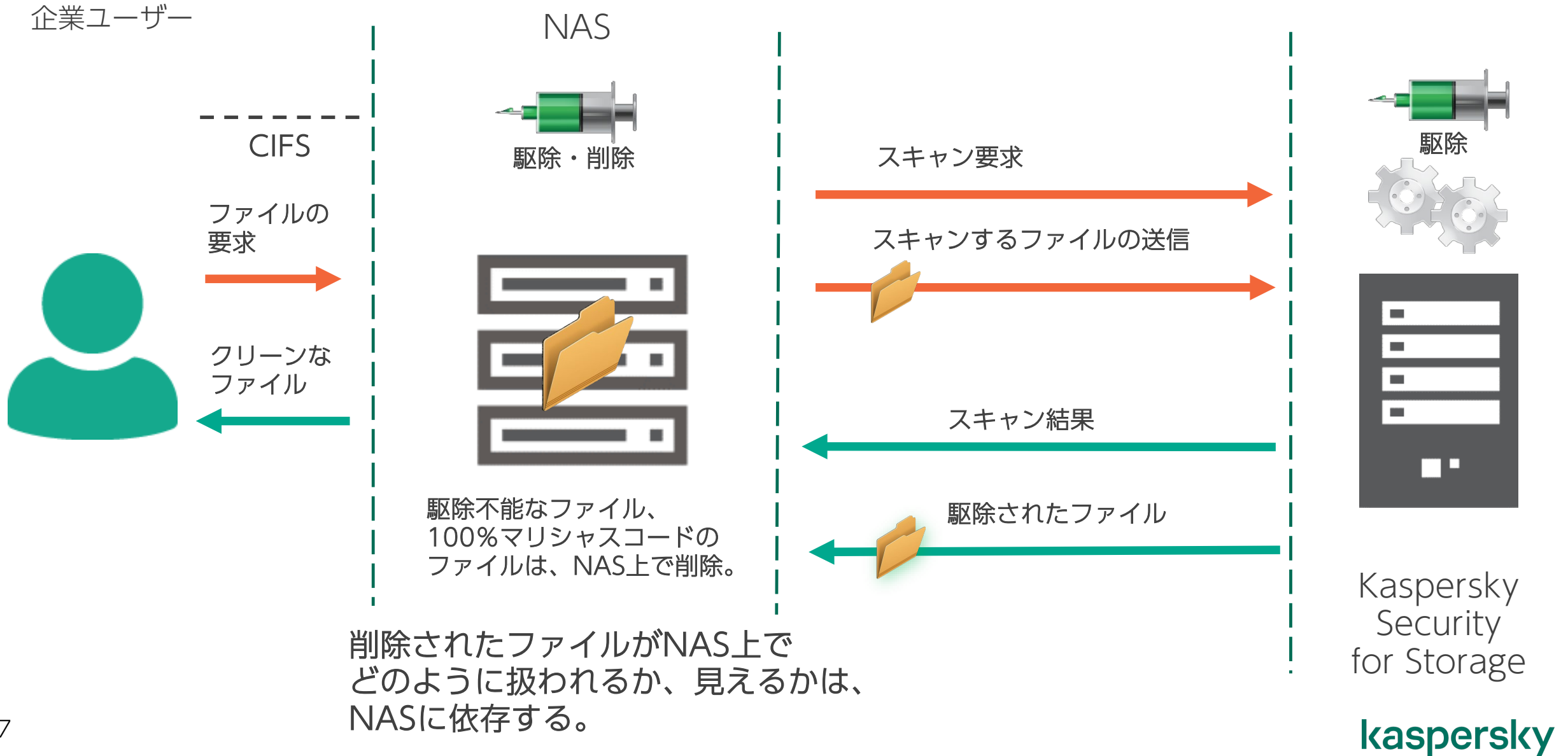


NASの共有域にアクセス

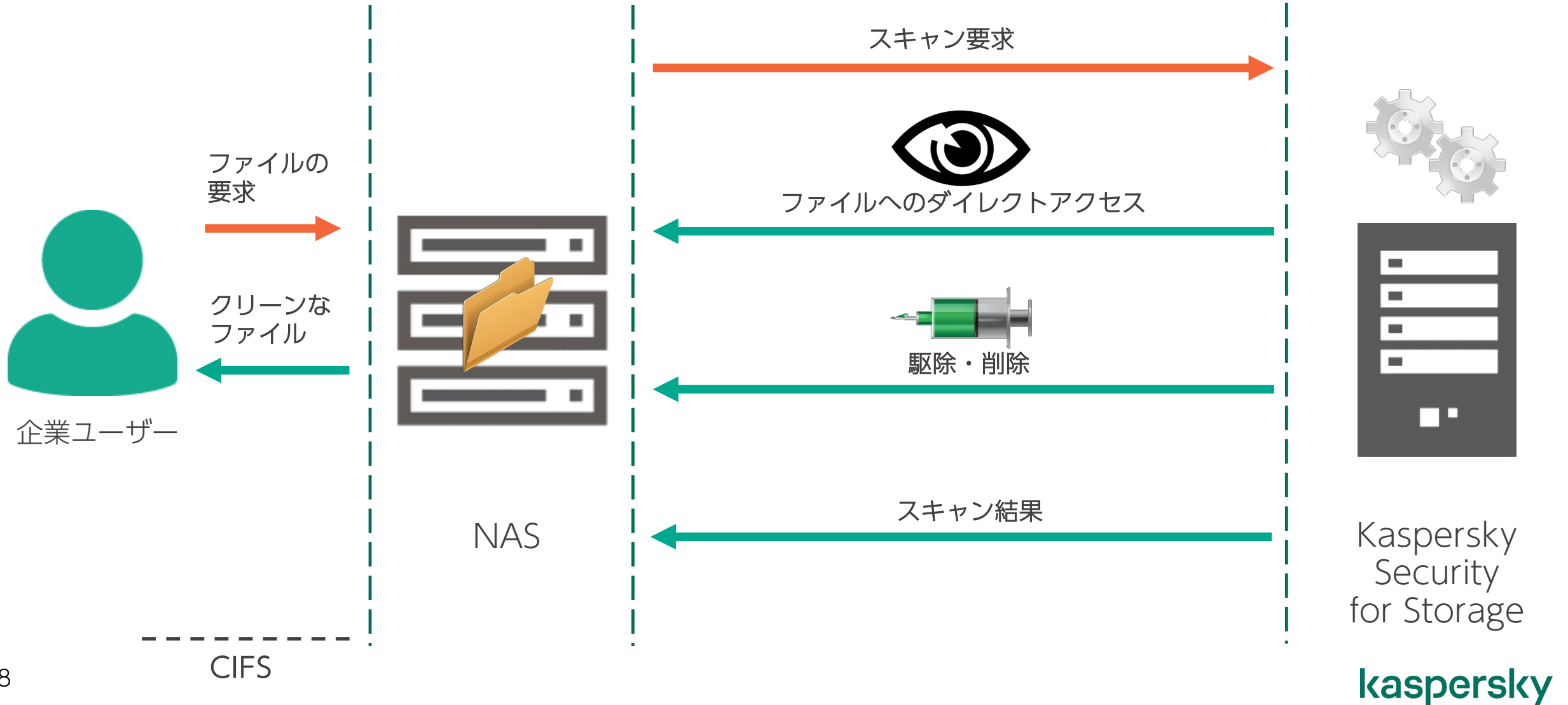


Windows Serverに、  
Kaspersky Security for Windows Serverをインストールし、  
Kaspersky Security for Storageライセンスでアクティベート

# ICAP (Internet Content Adaptation Protocol)



# RPC (remote procedure call)



## Kaspersky Security for Storage スキャンモード

オンアクセススキャンはユーザーのファイル操作が起点。  
オンデマンドスキャンはNASのスケジュール実行が起点。NASに機能がなければ実行できない。

### オンアクセススキャン

1. ユーザーがファイルをオープンや作成、変更しようとする。
2. NASが Kaspersky Security for Storageにファイルスキャンのために送信。
3. Kaspersky Security for Storage はファイルを処理し、NASに結果を通知。
4. Kaspersky Security for Storage のスキャン結果に従い、  
ユーザーはファイルへのアクセスを許可されるか、拒否される。

### オンデマンドスキャン

1. 管理者が、NAS上のオンデマンドスキャンタスクを追加し、実行する。
2. NASが Kaspersky Security for Storageにスキャンリクエストを送信
3. Kaspersky Security for Storage はファイルを処理し、NASに結果を通知。
4. NASはスキャン結果を記録する。



# Kaspersky Security for Storage 管理方法



kaspersky

# Kaspersky Security for Storageの管理

Kaspersky Security Center (KSC) による集中管理、  
Kaspersky Securityコンソールによるローカル管理、  
または、併用が可能。

併用の場合、KSCにロックをかけた項目を  
ローカルコンソールで変更することは出来ない。  
ロックしていない項目は、ローカル管理者に委ねられる。

# Kaspersky Security Center

シングルコンソールによる集中管理を可能にする、管理サーバー。  
様々なアプリケーションを管理。



**Kaspersky Security Center**  
企業インフラストラクチャー内の物理、仮想ノード、モバイル端末を管理。  
ポリシー・タスクによる管理、レポート、アラート。



Kaspersky Security for Business など



Kaspersky Security for Storage

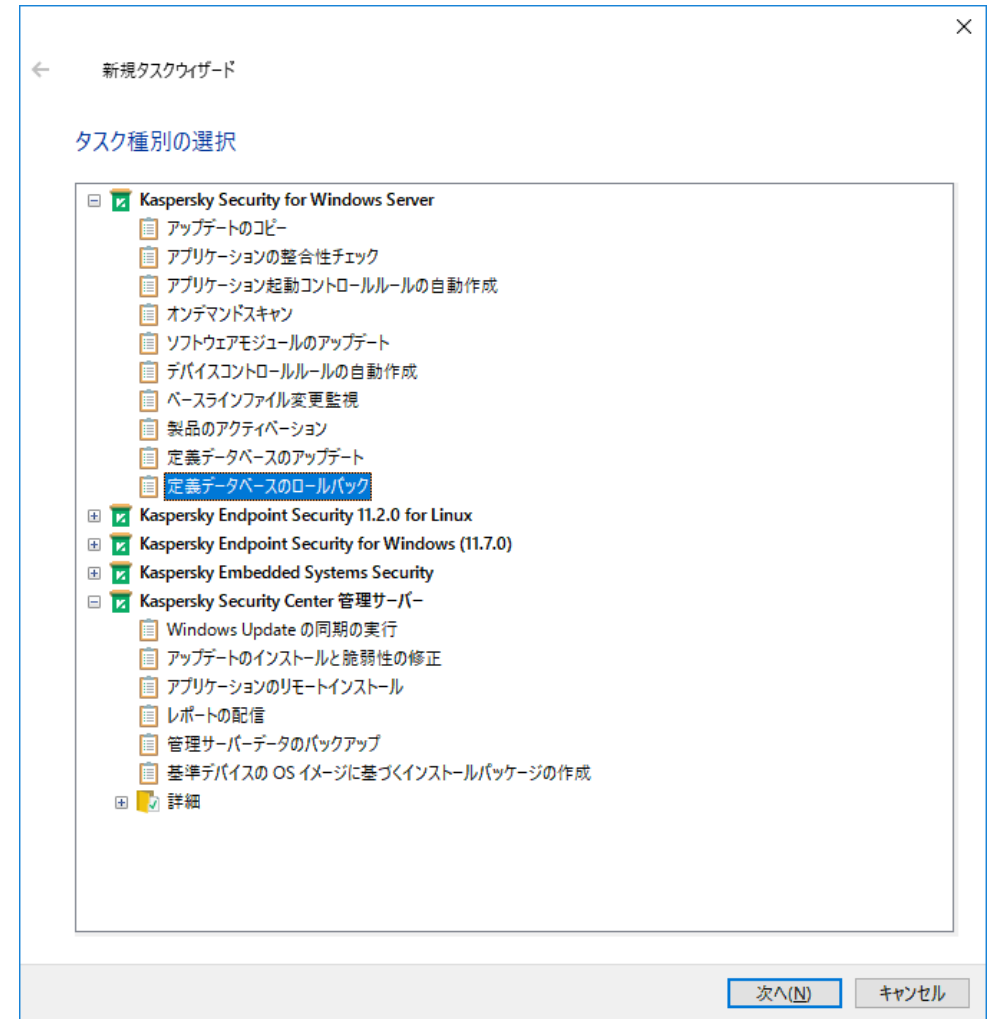
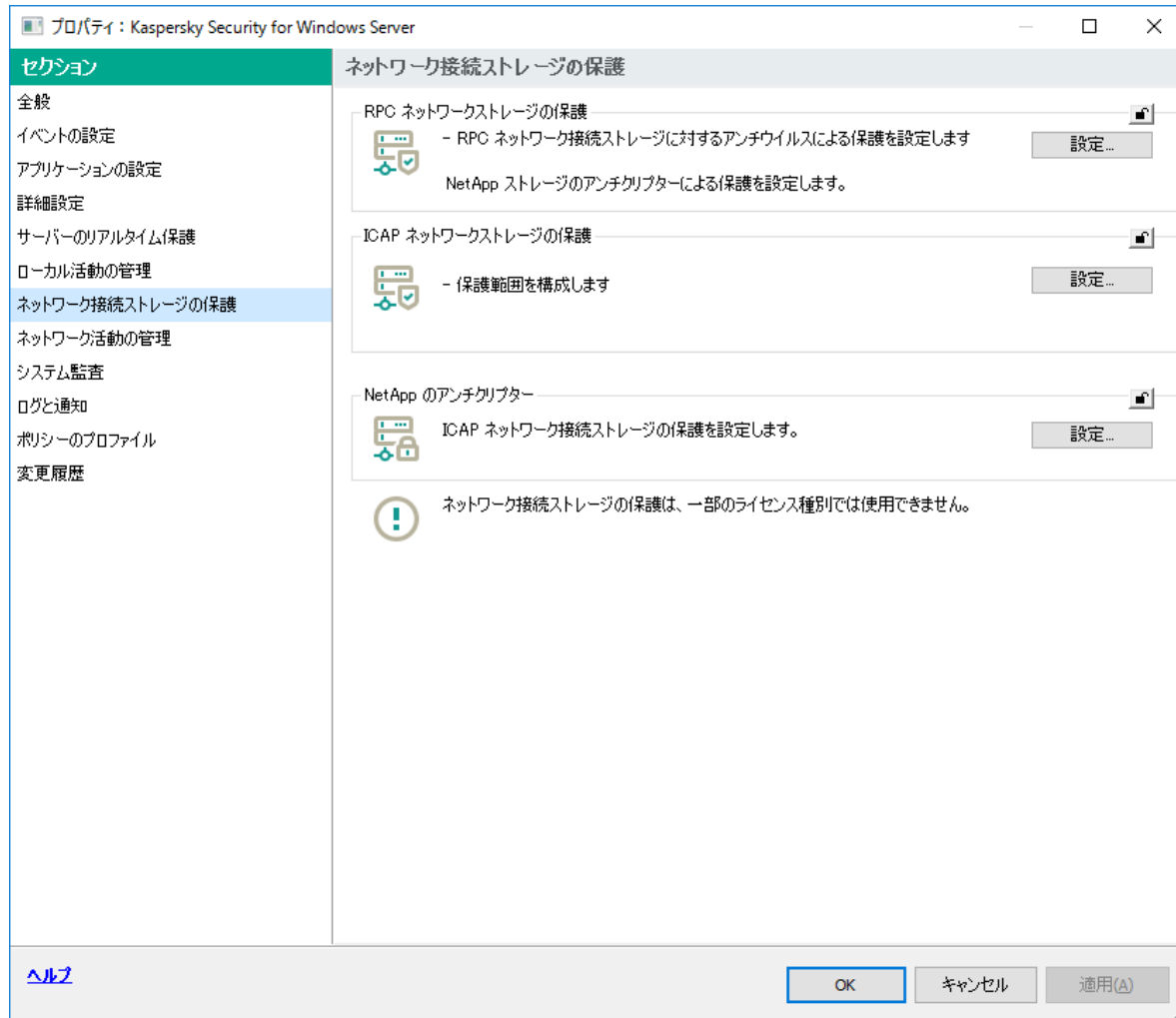
# Kaspersky Security Center

ポリシー・タスクによる一元管理、レポート。

The screenshot displays the Kaspersky Security Center 13 interface. The left sidebar shows a navigation tree with categories like '管理サーバー KSC', '管理対象デバイス', 'モバイルデバイス管理', 'ポリシー', 'タスク', and '詳細'. The main area is titled '管理サーバー KSC > 管理対象デバイス > for Storage'. Below this, there are tabs for 'デバイス', 'ポリシー', and 'タスク'. A table lists devices with columns for '名前', '前回の管理サ...', 'ネットワークエー...', 'リアルタイム...', '作成日', and 'OSのリリース ID'. The table contains two rows: KSW502 and KSW501. At the bottom left, it says 'グループ: 0, デバイス: 2'. The Kaspersky logo is in the bottom right corner.

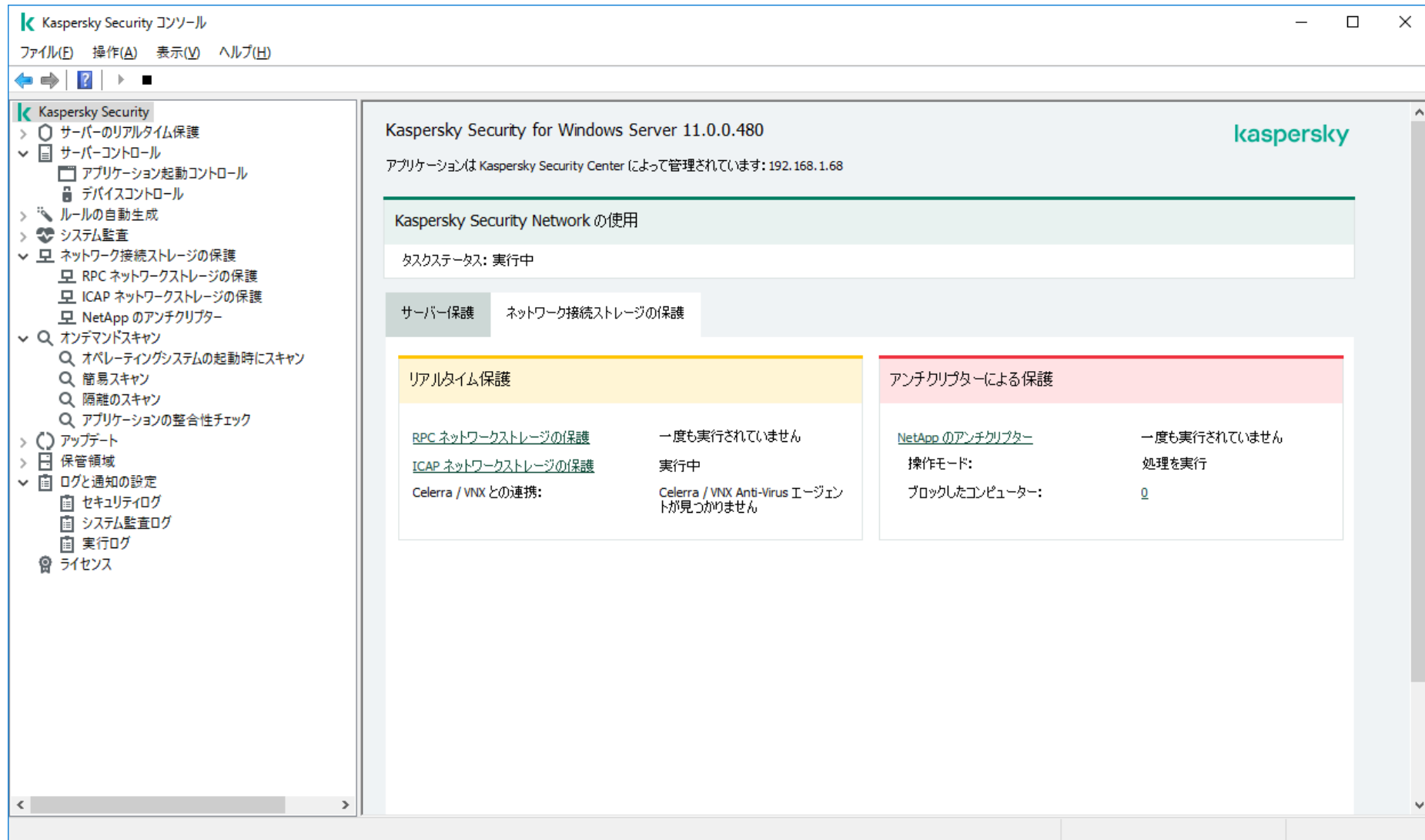
| 名前     | 前回の管理サ... | ネットワークエー... | リアルタイム... | 作成日  | OSのリリース ID |
|--------|-----------|-------------|-----------|------|------------|
| KSW502 | 7分前       | はい          | 実行中...    | 25分前 | 1607       |
| KSW501 | 1分前       | はい          | 実行中...    | 22分前 | 1607       |

# ポリシー・タスク



# Kaspersky Security コンソール

サーバー単位で管理。



# Kaspersky Security コンソール

## ポリシー・タスク

**Kaspersky Security コンソール**

ファイル(F) 操作(A) 表示(V) ヘルプ(H)

**Kaspersky Security**

- サーバーのリアルタイム保護
- サーバーコントロール
  - アプリケーション起動コントロール
  - デバイスコントロール
- ルールの自動生成
- システム監査
- ネットワーク接続ストレージの保護
  - RPC ネットワークストレージの保護
  - ICAP ネットワークストレージの保護**
  - NetApp のアンチクリプター
- オンデマンドスキャン
  - オペレーティングシステムの起動時にスキャン
  - 簡易スキャン
  - 隔離のスキャン
  - アプリケーションの整合性チェック
- アップデート
- 保管領域
- ログと通知の設定
  - セキュリティログ
  - システム監査ログ
  - 実行ログ
- ライセンス

### ICAP ネットワークストレージの保護

**管理**

タスクステータス: **実行中**

開始時刻: 2021/10/11 16:02:52

実行ログを開く

**プロパティ**

スケジュール: アプリケーションの起動時

次回開始: 未定義

ICAP サービス接続ポート: 1344  
ICAP サービス ID: avscan  
ヒューリスティックアナライザーを使用する: はい  
ヒューリスティック分析レベル: 中  
KSN サービスの使用: はい  
オブジェクトをスキャン: ファイル形式によってオブジェクトをスキャン  
アーカイブ: スキャンしない  
SFx アーカイブ: スキャンする  
メールデータベース: スキャンしない  
圧縮されたオブジェクト: スキャンする  
通常のメール: スキャンしない  
OLE 埋め込みオブジェクト: スキャンする

感染などの問題があるオブジェクトの処理: 推奨処理を実行  
感染の可能性のあるオブジェクトの処理: 推奨処理を実行

**プロパティ**

**プロパティ**

- 設定のエクスポート
- 設定のインポート

**更新**

- ヘルプ

**統計情報**

| 名前                  | 値 |
|---------------------|---|
| 検知                  | 0 |
| 感染などの問題があるオブジェクトの検知 | 0 |
| 感染の可能性のあるオブジェクトの検知  | 0 |
| 駆除されていないオブジェクト      | 0 |
| 隔離されていないオブジェクト      | 0 |
| スキャンされていないオブジェクト    | 0 |
| バックアップされていないオブジェクト  | 0 |
| 処理エラー               | 0 |
| 駆除されたオブジェクト         | 0 |
| 隔離済み                | 0 |
| バックアップ済み            | 0 |
| パスワードで保護されているオブジェクト | 0 |
| 破損しているオブジェクト        | 0 |
| 処理されたオブジェクト         | 0 |

### タスクの設定

全般 スケジュール 詳細設定

ICAP サービス接続設定

ネットワークポート番号: 1344

サービス ID: avscan

ヒューリスティックアナライザーを使用する

低 中 高

保護に KSN を使用する

セキュリティレベル

推奨

[推奨] セキュリティレベルは、カスペルスキーが最適なレベルとして推奨します。  
[推奨] セキュリティレベルに設定した場合:

- ファイル形式によってオブジェクトをスキャンします
- 自己解凍アーカイブをスキャンします
- 圧縮されたファイルをスキャンします
- OLE 埋め込みファイルをスキャンします
- 8 MB を超える複合ファイルをスキャンしません

設定...

ヘルプ

OK キャンセル

# 高度なセキュリティ機能



kaspersky



# 高度なセキュリティ機能

- ヒューリスティックによる検知
- KSNによる検知
- 定義のロールバック

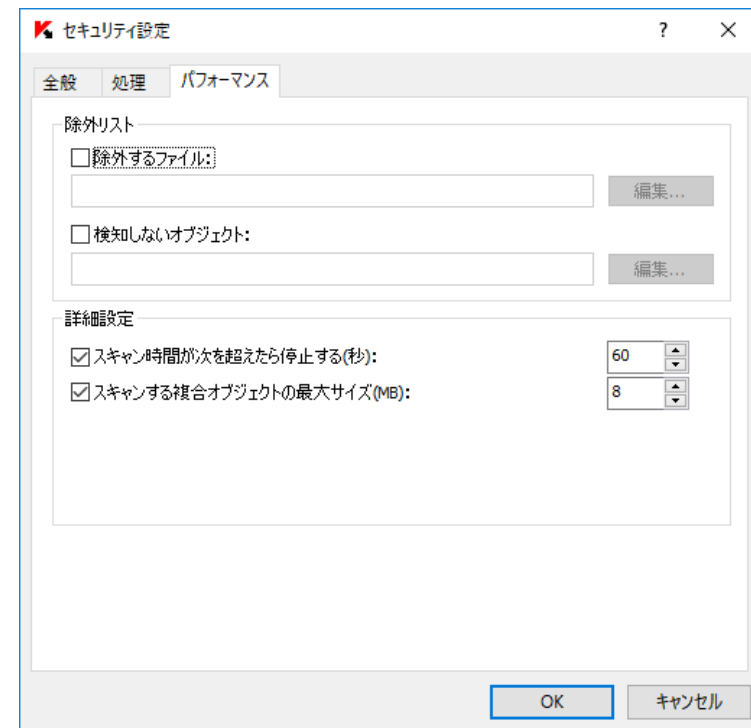
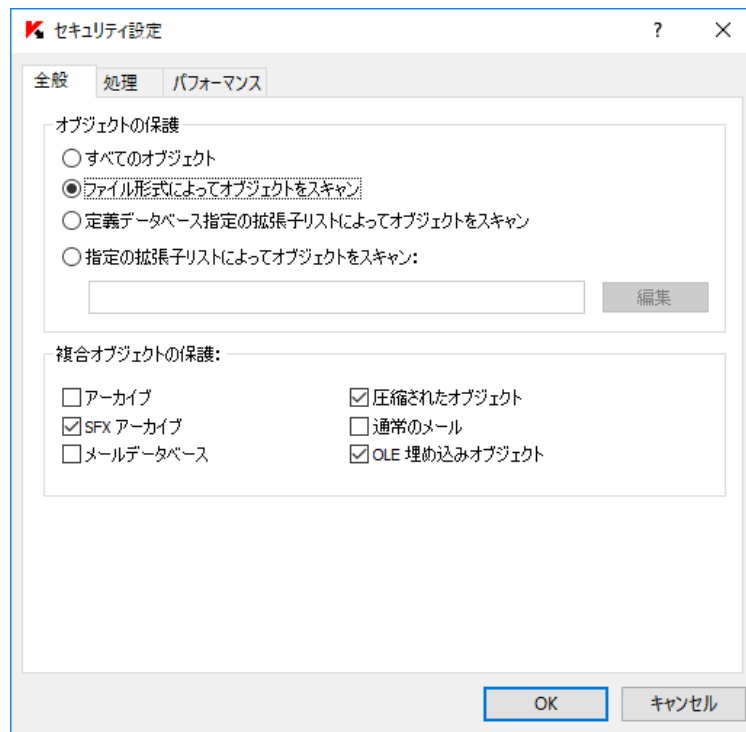
## • その他

### 最適化されたデフォルト設定

ファイル形式に基づいて、感染の可能性があるオブジェクトのみがスキャンされます。

### 除外設定

### スキャン上限の設定



# 高度なセキュリティ機能

## ヒューリスティック分析とは何か

既知の脅威を対象とする現在の定義データベースでは検知出来ない未知の脅威を検知する技術。

## 静的・動的解析

静的解析は、マルウェアに特徴的な疑わしいコードをスキャンし解析する

ヒューリスティックアナライザーは疑わしい痕跡が見つかる度にカウンターを増加させる。

動的解析は、特殊な仮想環境で対象のプログラムを実行し、疑わしい行為を発見したら、マルウェアと識別しブロックする。

# Kaspersky Security Networkによる高度なセキュリティ

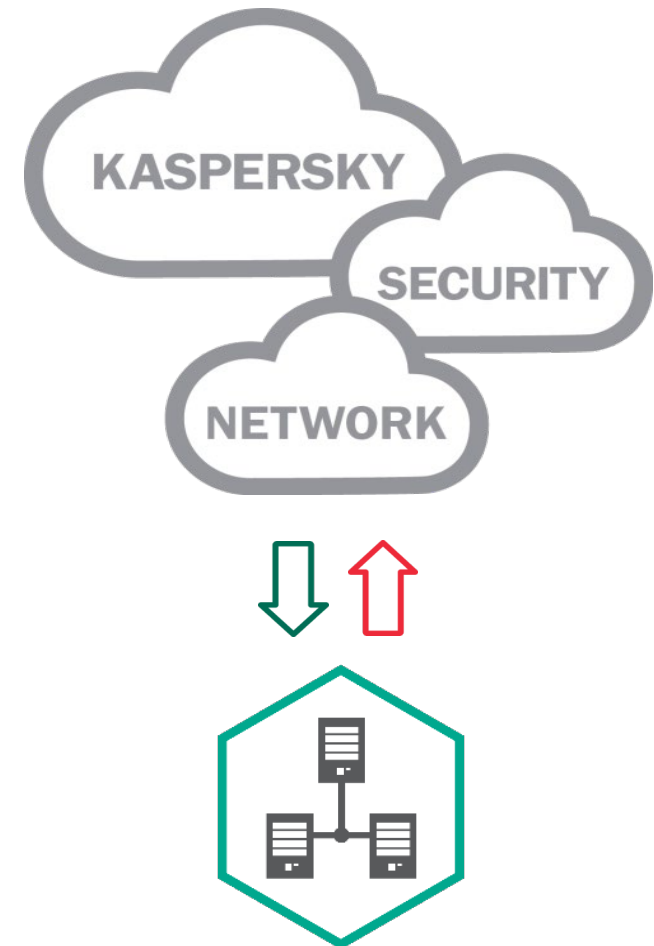
## KSNとは何か

最も高度であるグローバルな  
クラウドベースセキュリティネットワーク

動的なカテゴリイズとレピュテーション

リアルタイム保護を可能にする

カスペルスキーエンタープライズ製品との  
完全な統合



# 参考資料

## NASとの連携設定



kaspersky

# Isilon OneFS ICAP連携 設定画面


# Isilon OneFS ICAP連携のメリット

- リアルタイムスキャンとオンデマンドスキャン  
スキャン領域ごとのオンデマンドスキャンスケジュール設定
- KSN との統合・ヒューリスティック分析
- ローカルコンソールまたはKSCによる集中管理  
レポート、アラート、syslog、SIEM連携
- 拡張性と冗長性
- Isilon上へのマルウェア・疑わしいファイルの隔離

# OneFS ICAP設定

## 2台のKaspersky Security for Storageを設定

OneFS STORAGE ADMINISTRATION

Logged in as admin | [Review recent events](#) | [Log out](#) | [Help](#) 

Cluster name: ci-klj (OneFS version: 8.2.1.0) Node 1

Dashboard ▾ Cluster management ▾ File system ▾ Data protection ▾ Access ▾ Protocols ▾

### Antivirus

Policies Reports Detected threats **ICAP servers** Settings

#### ICAP servers

[+ Add an ICAP server](#)

Bulk actions ▾

| <input type="checkbox"/> | Server name                      | State   | Actions  |
|--------------------------|----------------------------------|---------|--|
| <input type="checkbox"/> | icap://192.168.1.163/avscan:1344 | Enabled | <a href="#">View / Edit</a> <a href="#">Delete</a> |
| <input type="checkbox"/> | icap://192.168.1.164/avscan:1344 | Enabled | <a href="#">View / Edit</a> <a href="#">Delete</a> |

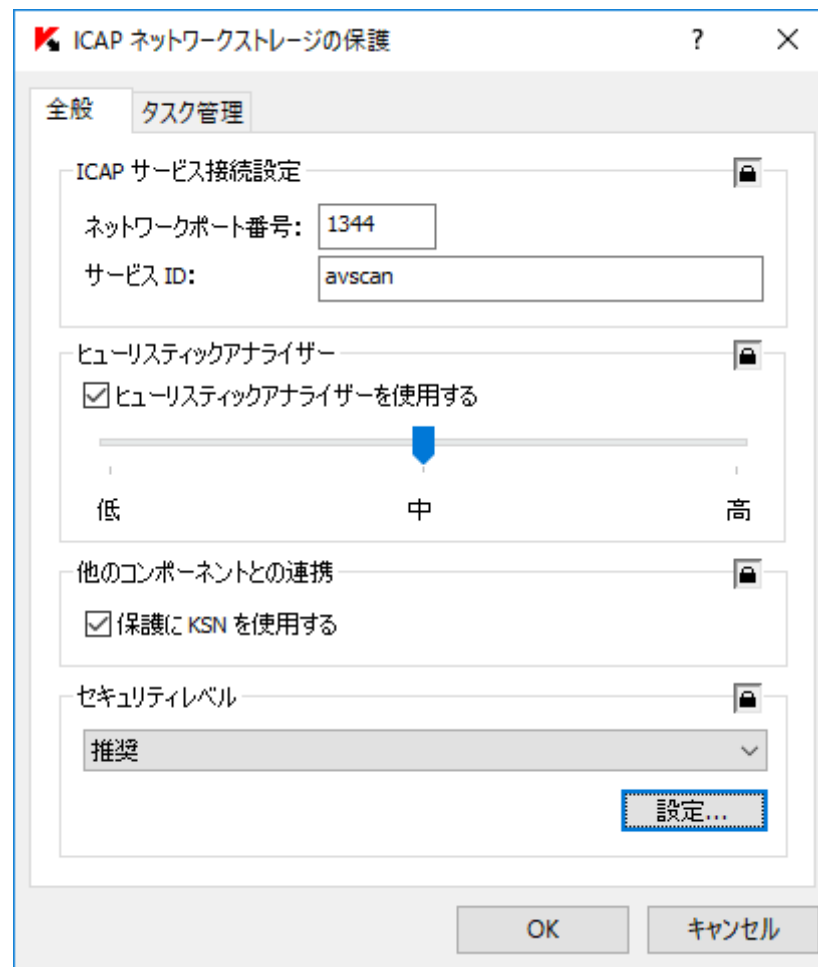
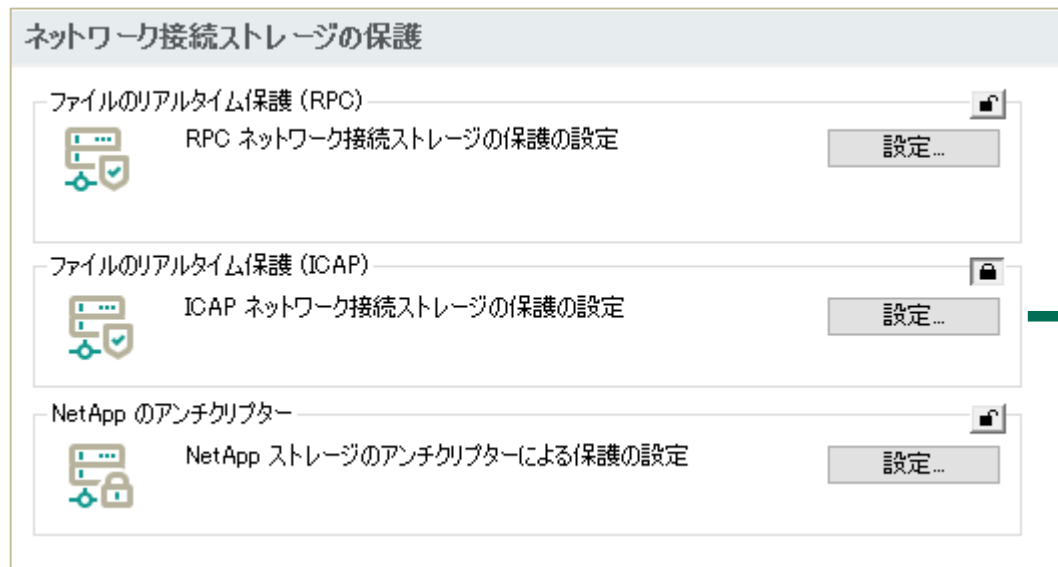
# OneFS ICAP設定 オンアクセス時スキャンによる検知

The screenshot displays the OneFS Storage Administration web interface. At the top, the OneFS logo and 'STORAGE ADMINISTRATION' are visible on the left, and the user 'admin' is logged in on the right. A navigation menu includes Dashboard, Cluster management, File system, Data protection, Access, and Protocols. The 'Antivirus' section is active, with sub-tabs for Policies, Reports, Detected threats, ICAP servers, and Settings. The 'Antivirus threat reports' table shows a list of detected threats, all identified as EICAR-Test-Files. The table columns are Name, Path, Remediation, Policy, Detected, and Actions. The detected times range from 16:34:47 to 16:43:18 on 2020-04-21.

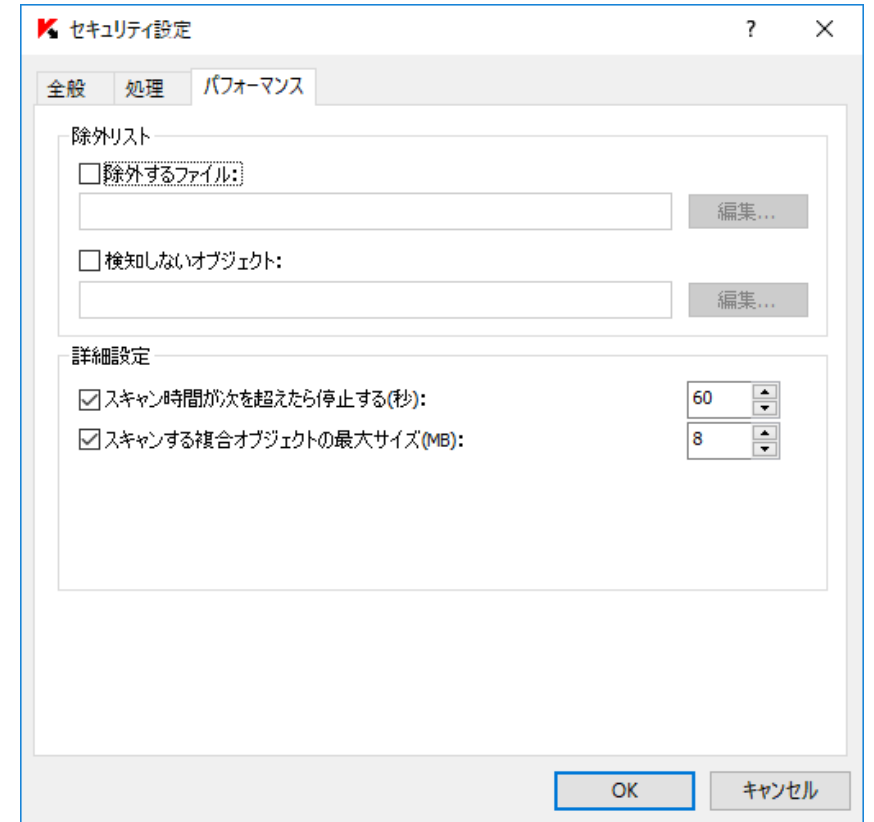
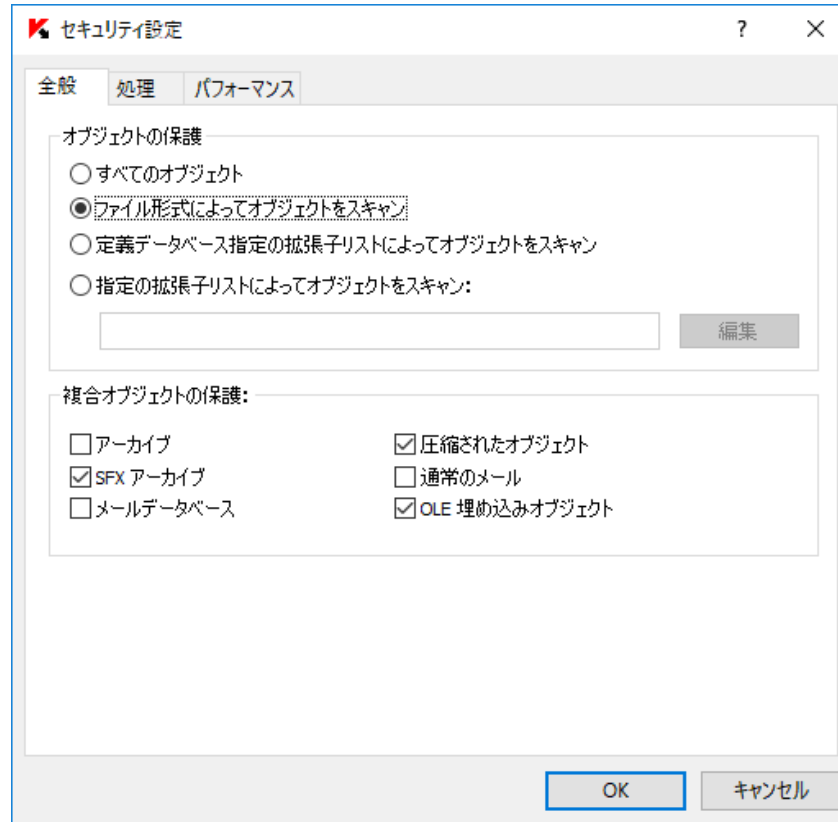
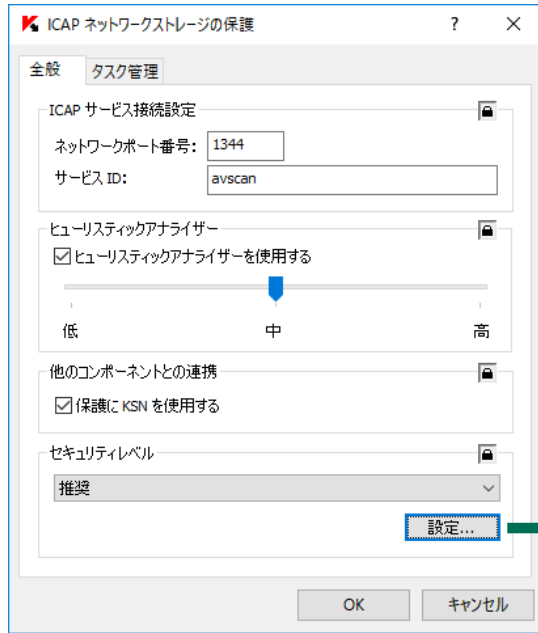
| Name            | Path   | Remediation | Policy        | Detected            | Actions           |
|-----------------|--|-------------|---------------|---------------------|-------------------|
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/新しいフォル...            | Quarantined | SCAN_ON_CLOSE | 2020-04-21 16:43:18 | View details More |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/新しいフォル...            | Quarantined | SCAN_ON_CLOSE | 2020-04-21 16:42:25 | View details More |
| EICAR-Test-File | /ifs/home/user01/eicarcom2/eicar_com/eicar.com | Quarantined | SCAN_ON_CLOSE | 2020-04-21 16:40:19 | View details More |
| EICAR-Test-File | /ifs/home/user01/eicar.com.txt                 | Quarantined | SCAN_ON_OPEN  | 2020-04-21 16:39:27 | View details More |
| EICAR-Test-File | /ifs/home/user01/eicar.com                     | Quarantined | SCAN_ON_CLOSE | 2020-04-21 16:39:20 | View details More |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/eicar.com            | Quarantined | SCAN_ON_CLOSE | 2020-04-21 16:35:29 | View details More |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/eicar.com.txt        | Quarantined | SCAN_ON_OPEN  | 2020-04-21 16:34:47 | View details More |



# Kaspersky Security for Storage ICAP設定



# Kaspersky Security for Storage ICAP設定 詳細



# OneFS ICAP設定 スケジュールスキャン設定 (オンデマンドスキャン)

OneFS STORAGE ADMINISTRATION

Logged in as admin | [Review recent events](#) | [Log out](#) | [Help](#) ?

Cluster name: cl-klj (OneFS version: 8.2.1.0) Node 1

Dashboard ▾ Cluster management ▾ File system ▾ Data protection ▾ Access ▾ Protocols ▾

## Antivirus

Policies Reports Detected threats ICAP servers Settings

### Antivirus policies

[+ Create an antivirus policy](#)

Bulk actions ▾

| <input checked="" type="checkbox"/> | Policy name | State   | Last successful job | Schedule | Actions  |
|-------------------------------------|-------------|---------|---------------------|----------|--|
| <input checked="" type="checkbox"/> | AV Policy   | Enabled | Yesterday           | Manual   | <a href="#">View / Edit</a>   <a href="#">More ▾</a> |

アンチウイルスポリシーを作成し、  
スケジュール起動、手動起動によるフォルダー単位スキャンを可能とする

# OneFS ICAP設定 スケジュールスキャン設定

アンチウイルスポリシー設定  
パスやスケジュールの指定

**Edit antivirus policy details** Help ?

\* = Required field

**Settings**

Enable antivirus policy

\* Policy name  
AV Policy

Description

**Paths**

/ifs/home/user01

**Recursion depth**

Full recursion  
 Limit depth

**Schedule settings**

Enable force run of policy regardless of impact policy

Impact policy  
DEFAULT

**Schedule**

Manual  
 Scheduled

**Details**

Last-known good  
Yesterday

Policy ID  
180670b2b27e280

**Edit antivirus policy details** Help ?

\* = Required field

**Recursion depth**

Full recursion  
 Limit depth

**Schedule settings**

Enable force run of policy regardless of impact policy

Impact policy  
DEFAULT

**Schedule**

Manual  
 Scheduled

Weekly

**Weekly schedule**

Run policy every: 1 week(s)

Run policies on:

|                                    |  |
|------------------------------------|--|
| <input type="checkbox"/> Monday    | <input type="checkbox"/> Friday            |
| <input type="checkbox"/> Tuesday   | <input type="checkbox"/> Saturday          |
| <input type="checkbox"/> Wednesday | <input checked="" type="checkbox"/> Sunday |
| <input type="checkbox"/> Thursday  |  |

Run one policy per specified day

Run policy at: 12:00 PM

Run multiple policies per specified day

**Details**

Last-known good  
Yesterday

# OneFS ICAP設定

## スケジュールスキャンポリシー実行 (run)でのスキャンによる検知

The screenshot displays the OneFS Storage Administration web interface. At the top, it shows the user is logged in as 'admin' and provides links for 'Review recent events', 'Log out', and 'Help'. The cluster name is 'cl-klj (OneFS version: 8.2.1.0) Node 1'. The navigation menu includes 'Dashboard', 'Cluster management', 'File system', 'Data protection', 'Access', and 'Protocols'. The 'Antivirus' section is active, with sub-tabs for 'Policies', 'Reports', 'Detected threats', 'ICAP servers', and 'Settings'. The 'Antivirus threat reports' table is shown with a filter set to 'Filter by remediation' and a 'Reset' button. The table lists several detected threats, all identified as 'EICAR-Test-File' with a remediation status of 'Truncated'.

| Name            | Path  | Remediation | Policy          | Detected            | Actions             |
|-----------------|---|-------------|-----------------|---------------------|---------------------|
| EICAR-Test-File | /ifs/home/user01/eicar.com.txt                  | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:06 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/新しいフ...               | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:05 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/eicar.com.txt         | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:05 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/新しいフ...               | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:04 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/新しいフォルダー/eicar.com             | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:03 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/eicarcom2/eicar_com/eicar.c... | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:02 | View details More ▾ |
| EICAR-Test-File | /ifs/home/user01/eicar.com                      | Truncated   | 180670b2b27e280 | 2020-04-21 16:50:02 | View details More ▾ |

# Oracle ZFS ICAP連携 設定画面



構成

保守

シェア

ステータス

分析

サービス

ストレージ

ネットワーク

SAN

クラスタ

ユーザー

プリファレンス

SETTINGS

アラート

サービス

データサービス

|   |       |                    |  |  |
|---|-------|--------------------|--|--|
| <input checked="" type="radio"/> NFS          | オンライン | 2021-2-27 02:07:37 |  |  |
| <input checked="" type="radio"/> iSCSI        | オンライン | 2021-2-27 01:54:40 |  |  |
| <input checked="" type="radio"/> SMB          | オンライン | 2021-2-27 02:06:30 |  |  |
| <input type="radio"/> FTP                     | 無効    | 2021-2-27 01:46:36 |  |  |
| <input type="radio"/> HTTP                    | 無効    | 2021-2-27 01:46:36 |  |  |
| <input checked="" type="radio"/> NDMP         | オンライン | 2021-2-27 01:54:45 |  |  |
| <input checked="" type="radio"/> リモートレプリケーション | オンライン | 2021-2-27 01:54:31 |  |  |
| <input checked="" type="radio"/> シャドウ移行       | オンライン | 2021-2-27 01:54:40 |  |  |
| <input type="radio"/> SFTP                    | 無効    | 2021-2-27 01:46:37 |  |  |
| <input type="radio"/> SRP                     | 無効    | 2021-2-27 01:46:38 |  |  |
| <input type="radio"/> TFTP                    | 無効    | 2021-2-27 01:54:40 |  |  |
| <input type="radio"/> ウィルススキャン                | 無効    | 2021-2-27 01:46:38 |  |  |

サービス
ウイルススキャン
プロパティ
ログ

サービスに戻る
2021-2-27 02:10:24 オンライン
元に戻す
適用

**ウイルススキャン**  
 ウイルススキャンをファイルシステムのレベルで構成します。ウイルススキャンを有効にするには、メインナビゲーションから「シェア」を選択し、ファイルシステムまたはプロジェクトを編集して「一般」を選択します。

**関連項目**  
[ヘルプ: ウイルススキャン](#)  
[ウィキペディア: ウイルス対策](#)

スキャンする最大ファイルサイズ  G   
 最大ファイルサイズを超えるファイルへのアクセスを許可

**ファイル拡張子**  
 拡張子でスキャンするファイルを指定してください。ワイルドカードの "\*" と "?" を使用すると、それぞれ任意の文字セットまたは任意の 1 字に一致します。

| アクション                             | パターン                           |
|-----------------------------------|--------------------------------|
| <input type="text" value="スキャン"/> | <input type="text" value="*"/> |

**スキャンエンジン**

| 有効                                  | ホスト  | 最大接続                            | ポート                               |
|-------------------------------------|--|---------------------------------|-----------------------------------|
| <input checked="" type="checkbox"/> | <input type="text" value="192.168.1.164"/> | <input type="text" value="32"/> | <input type="text" value="1344"/> |

ICAPの指定やサービスIDの指定は無し。



pool01/local/default/test

元に戻す 適用

**使用状況** 0.1%/19.6G  
 参照されているデータ 11.5M  
 合計領域 11.5M

**静的プロパティ**  
 作成日 2021-2-27  
 圧縮 1.00x  
 大文字と小文字の区別 混在  
 非 UTF-8 を拒否 はい  
 正規化 なし  
 暗号化 オフ  
 Effective read limit unlimited  
 Effective write limit unlimited

**領域の使用**

データ

割り当て制限  0 G  
 スナップショットを含める  
 予約  0 G  
 スナップショットを含める

ユーザーとグループ

ユーザーまたはグループ  [すべて表示](#)

使用状況 none

割り当て制限  なし  デフォルト  
 0 G

**Bandwidth**

Read limit  unlimited  デフォルト  
 0 G/s  
 Write limit  unlimited  デフォルト  
 0 G/s

**プロパティ**

プロジェクトから継承

マウントポイント   
 読み取り専用   
 読み取り時のアクセス時間の更新   
 非ブロックの必須ロック   
 データ複製解除 (warning)   
 データ圧縮   
 チェックサム   
 キャッシュデバイスの使用状況   
 同期書き込みバイアス   
 データベースのレコードサイズ   
 追加レプリケーション   
 ウイルススキャン   
 破棄の防止   
 所有権の変更の制限

Kaspersky Security コンソール

ファイル(E) 操作(A) 表示(V) ヘルプ(H)

Kaspersky Security

- サーバーのリアルタイム保護
  - ファイルのリアルタイム保護 (ポリシーによって管理がブロックされている)
  - KSN の使用 (ポリシーによって管理がブロックされている)
  - ネットワーク脅威対策 (ポリシーによって管理がブロックされている)
  - トラフィックセキュリティ (ポリシーによって管理がブロックされている)
  - アンチクリプター
- サーバーコントロール
  - ルールの自動生成
  - システム監査
- ネットワーク接続ストレージの保護
  - RPC ネットワークストレージの保護
  - ICAP ネットワークストレージの保護
  - NetApp のアンチクリプター
- オンデマンドスキャン
- アップデート
- 保管領域
  - 隔離
  - バックアップ
  - ブロック対象コンピューターの保管領域
- ログと通知の設定
  - セキュリティログ
  - システム監査ログ
  - 実行ログ
  - ライセンス

### ICAP ネットワークストレージの保護

**管理**

タスクステータス: **実行中**  
停止

開始時刻: 2021/02/26 17:41:21  
実行ログを開く

**プロパティ**

スケジュール: アプリケーションの起動時  
次回開始: 未定義

ICAP サービス接続ポート: 1344  
ICAP サービス ID: avscan  
ヒューリスティックアナライザーを使用する: はい  
ヒューリスティック分析レベル: 中  
KSN サービスの使用: はい  
オブジェクトをスキャン: ファイル形式によってオブジェクトをスキャン  
アーカイブ: スキャンしない  
SFX アーカイブ: スキャンする  
メールデータベース: スキャンしない  
圧縮されたオブジェクト: スキャンする  
通常のメール: スキャンしない  
OLE 埋め込みオブジェクト: スキャンする

感染などの問題があるオブジェクトの処理: 推奨処理を実行  
感染の可能性のあるオブジェクトの処理: 推奨処理を実行

プロパティ

**プロパティ**

- プロパティ
- 設定のエクスポート
- 設定のインポート

更新  
ヘルプ

**統計情報**

| 名前                  | 値   |
|---------------------|-----|
| 検知                  | 4   |
| 感染などの問題があるオブジェクトの検知 | 9   |
| 感染の可能性のあるオブジェクトの検知  | 35  |
| 駆除されていないオブジェクト      | 3   |
| 隔離されていないオブジェクト      | 2   |
| スキャンされていないオブジェクト    | 0   |
| バックアップされていないオブジェクト  | 0   |
| 処理エラー               | 1   |
| 駆除されたオブジェクト         | 0   |
| 隔離済み                | 33  |
| バックアップ済み            | 9   |
| パスワードで保護されているオブジェクト | 0   |
| 破損しているオブジェクト        | 1   |
| 処理されたオブジェクト         | 194 |

サービスIDは空欄にしなくてもOK。

K タスクの設定

全般 | スケジュール | 詳細設定

ICAP サービス接続設定

ネットワークポート番号: 1344

サービス ID: avscan

ヒューリスティックアナライザーを使用する

低 中 高

保護に KSN を使用する

セキュリティレベル

推奨

[推奨] セキュリティレベルは、カスペルスキーが最適なレベルとして推奨します。  
[推奨] セキュリティレベルに設定した場合は:

- ファイル形式によってオブジェクトをスキャンします
- 自己解凍アーカイブをスキャンします
- 圧縮されたファイルをスキャンします
- OLE 埋め込みファイルをスキャンします
- 8 MB を超える複合ファイルをスキャンしません

設定...

ヘルプ

OK キャンセル

ウイルススキャン

ウイルススキャンをファイルシステムのレベルで構成します。ウイルススキャンを有効にするには、メインナビゲーションから「シェア」を選択し、ファイルシステムまたはプロジェクトを編集して「一般」を選択します。

関連項目

ヘルプ: ウイルススキャン  
 ウィキペディア: ウイルス対策

スキャンする最大ファイルサイズ  G

最大ファイルサイズを超えるファイルへのアクセスを許可

ファイル拡張子

拡張子でスキャンするファイルを指定してください。ワイルドカードの "\*" と "?" を使用すると、それぞれ任意の文字セットまたは任意の 1 字に一致します。

| アクション   | パターン |
|---------|------|
| スキャン    | *    |
| スキャンしない | zzz  |
| スキャンしない | yyy  |

ICAPサーバーに送信しない除外設定。

スキャンエンジン

| 有効                                  | ホスト           | 最大接続 | ポート  |
|-------------------------------------|---------------|------|------|
| <input checked="" type="checkbox"/> | 192.168.1.163 | 32   | 1344 |
| <input checked="" type="checkbox"/> | 192.168.1.164 | 32   | 1344 |

検知後、ファイルはCIFS上に表示されるが、  
ロックされコピーや実行は出来ない。

The image shows a Windows File Explorer window with the address bar set to 192.168.1.60 > test. The file list contains:

| 名前                 | 更新日時            | 種類             |
|--------------------|-----------------|----------------|
| 新しいフォルダー           | 2021/02/27 2:26 | ファイル フォルダ      |
| eicar              | 2021/02/27 3:07 | MS-DOS バッチファイル |
| HEUR_VIRUS-KSN_BAD | 2021/02/27 3:08 | アプリケーション       |

A dialog box titled 'ファイル アクセスの拒否' (File Access Denied) is overlaid on the right. It contains the following text:

この操作を実行するアクセス許可が必要です。  
このファイルを変更するには、KLU\Administrator からアクセス許可を得る必要があります。

File details shown in the dialog:

- HEUR\_VIRUS-KSN\_BAD
- 種類: アプリケーション
- サイズ: 48.0 KB
- 更新日時: 2021/02/27 3:08

Buttons: 再試行(R) (Retry), キャンセル (Cancel), 詳細情報 (Details)

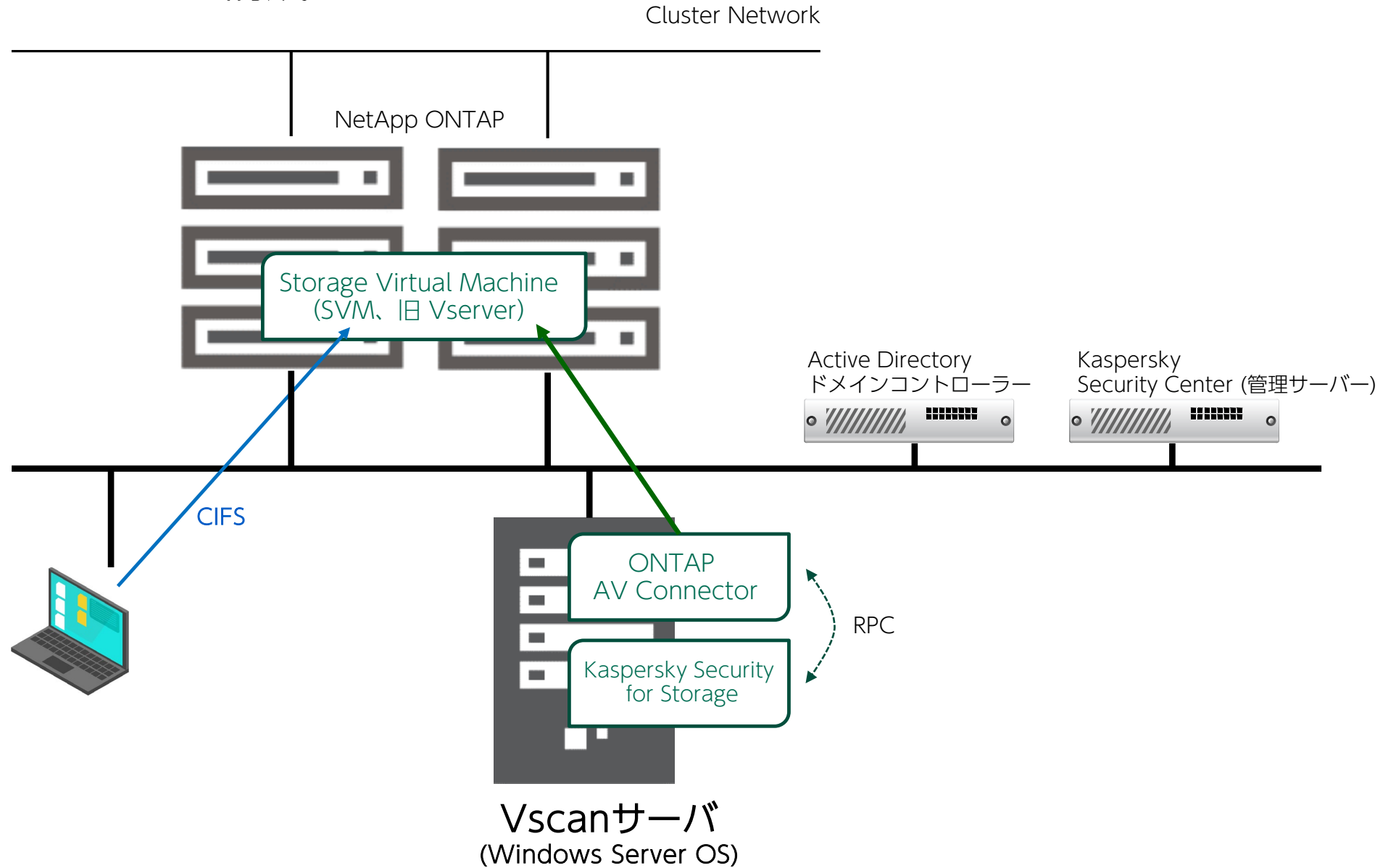
NetApp

## NetAppへ実装可能なセキュリティ

- リアルタイムスキャン (CIFS)
- オンデマンドスキャン (CIFS)
- アンチクリプター (CIFS、 対ランサムウェア)

NetApp fpolicyとKaspersky Security for Storage アンチクリプタータスクを使用

# NetApp Data ONTAP 構成



# NetAppにおけるオンデマンドスキャン

ONTAPにて、オンデマンドスキャンタスクを作成

オンデマンド タスクはオンデマンド スキャンの範囲を定義  
スキャンするファイルの最大サイズ、  
スキャン対象に含めるファイルの拡張子とパス、  
スキャン対象から除外するファイルの拡張子とパス

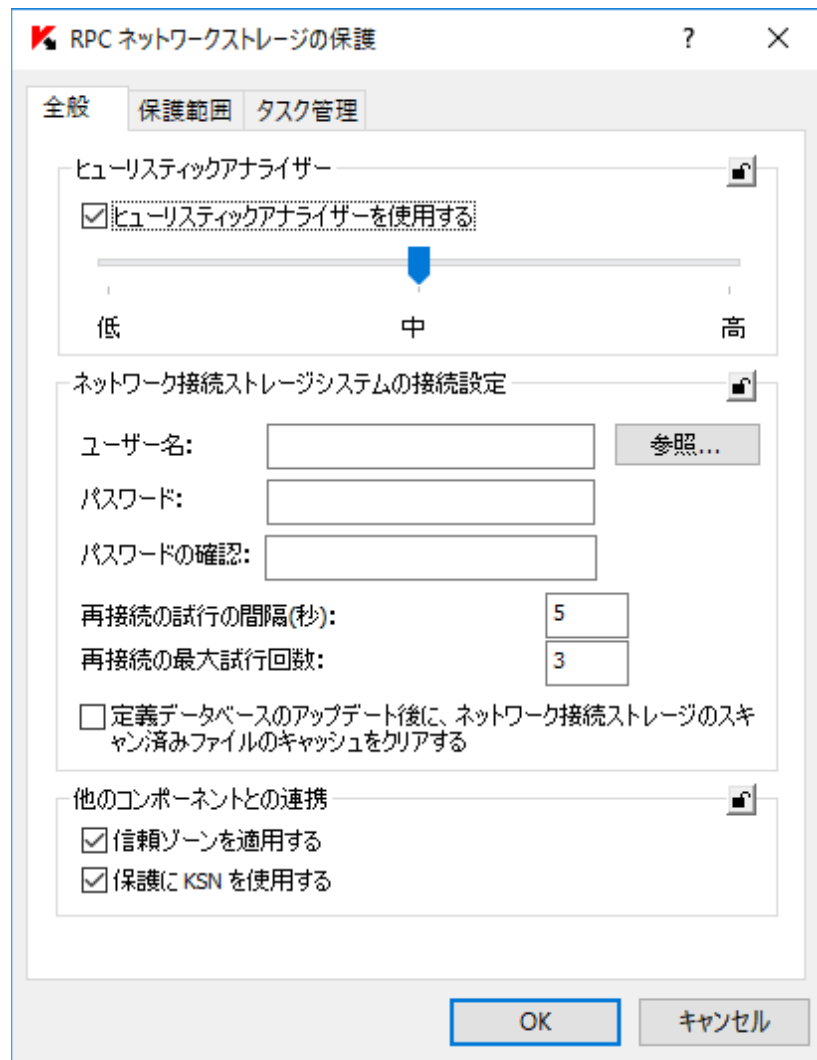
デフォルトでは、サブディレクトリ内のファイルもスキャンされる

vserver vscan on-demand-task runコマンドで、即時実行も可能

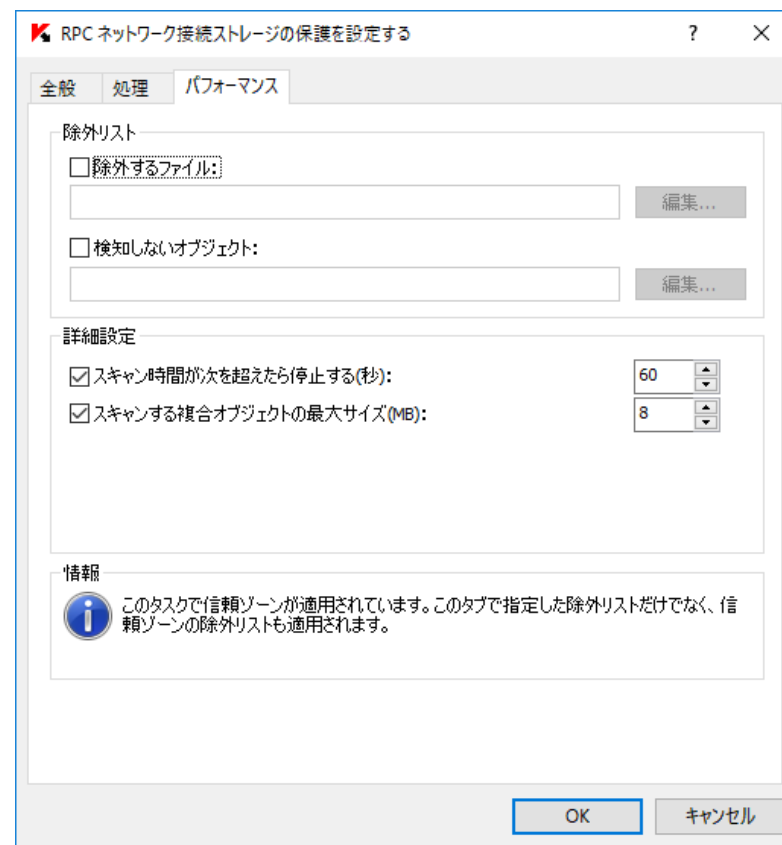
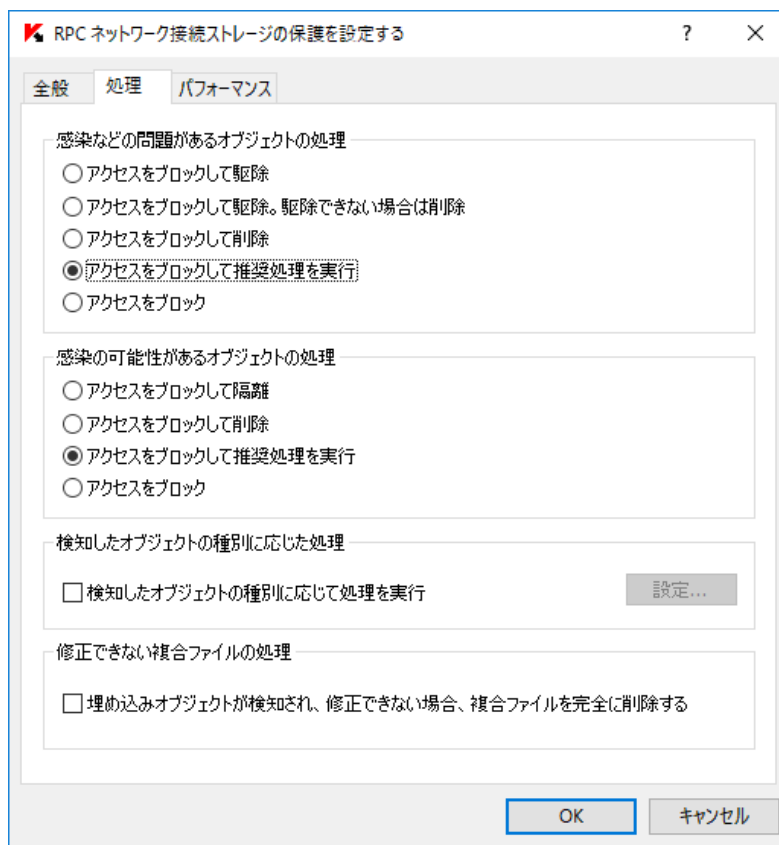
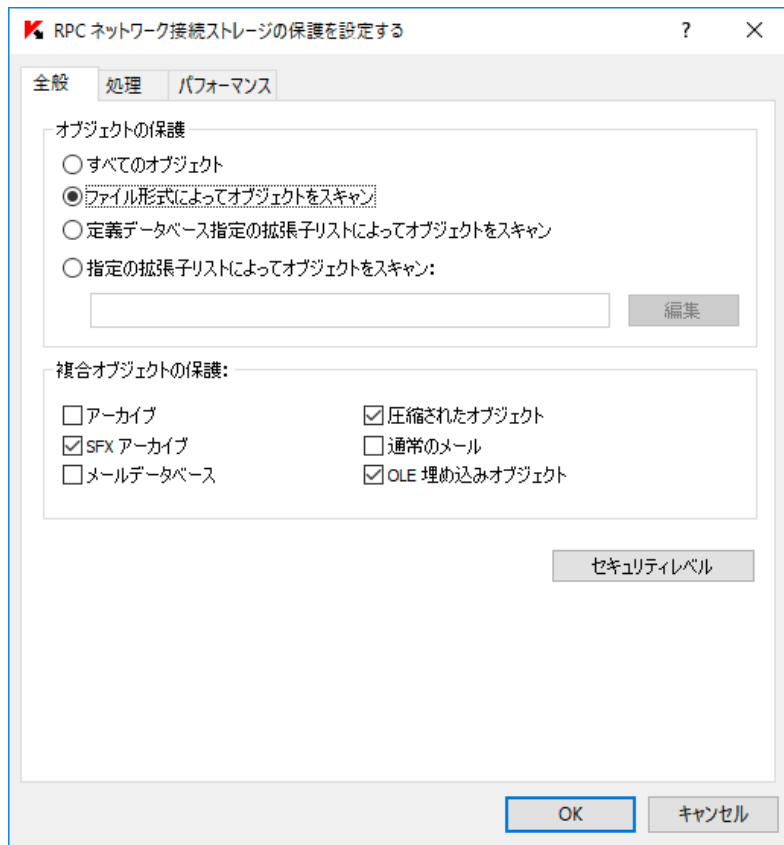


# Kaspersky Security for Storage

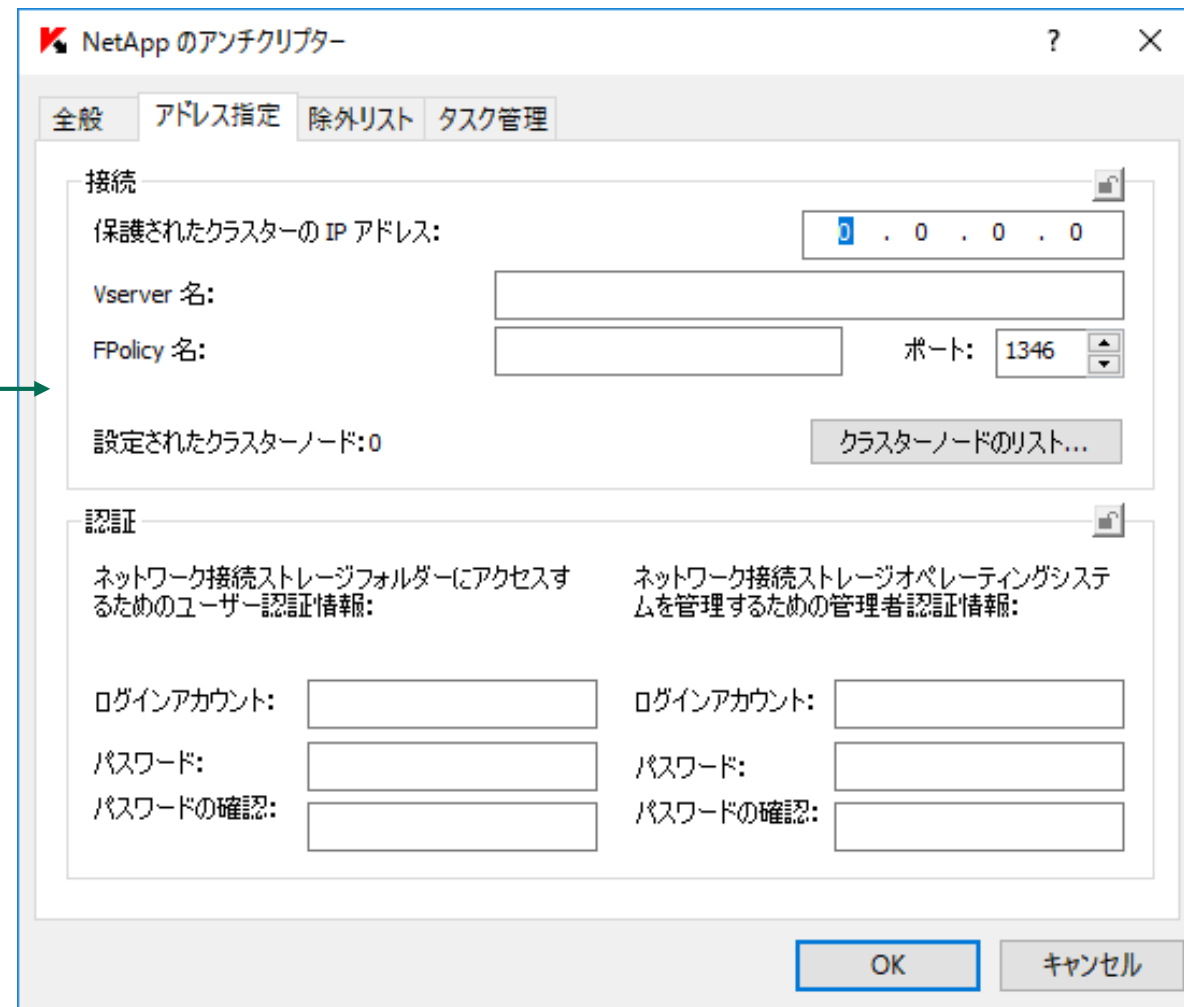
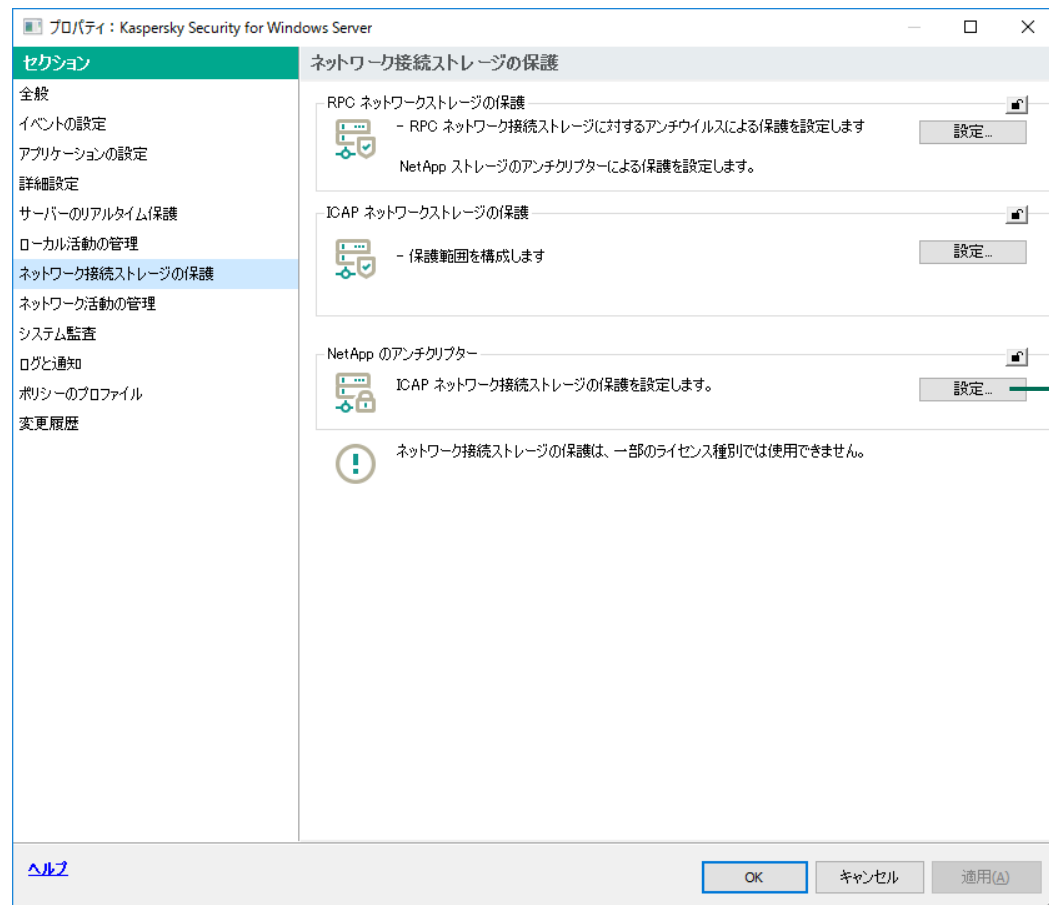
## RPC用設定詳細



# Kaspersky Security for Storage RPC用設定詳細



# Kaspersky Security for Storage NetApp アンチクリプター 設定詳細



# Kaspersky Security for Storage

## NetApp アンチクリプター 設定詳細

除外設定

下のタブで除外に複数の基準を設定できます。それらの基準は論理 AND で結合されます。

パス IP アドレス ユーザー

パスのマスクで除外:

▼ 追加

削除

| ルール名 |
|------|
|------|

OK キャンセル

除外設定

下のタブで除外に複数の基準を設定できます。それらの基準は論理 AND で結合されます。

パス IP アドレス ユーザー

クライアントコンピューターの IP アドレスで除外:

▼ 追加

削除

| ルール名 |
|------|
|------|

OK キャンセル

除外設定

下のタブで除外に複数の基準を設定できます。それらの基準は論理 AND で結合されます。

パス IP アドレス ユーザー

ユーザーで除外:

▼ 追加

削除

| ルール名 |
|------|
|------|

OK キャンセル