Microsoft

Microsoft Windows Server 2008 ネットワークアクセス保護（NAP） ログ監査ガイド

ホワイトペーパー

発行日 : 2008 年 6 月 23 日
最新の情報　http://www.microsoft.com/ja/jp/

注意事項：

マイクロソフト（米国 Microsoft Corporation、及び同社が直接または間接に所有する法人を含みます。以下同じ。）は、本書の内容及び本書を使用した結 果について明示的にも黙示的にも一切の保証を行いません。また、マイクロソフトは、本書を使用した結果に関し、（i）金融商品取引法、税法その他関係法令の遵守、（ii）その正確性、完全性及びその他の一切について、当該利用者及びその組織に対し、直接間接を問わず、いかなる責任も負担するものではありません。

お客様ご自身の責任において、 適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。 ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。

ただしこれは、著作権法上のお客様の権利を制限するものではありません。 マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の知的財産に関する権利をお客様に許諾するものではありません。

Microsoft、Windows、 Windows ロゴ、および Windows Server は米国 Microsoft Corporation の米国またはその他の国における登録商標または商標です。

このドキュメントに記載されている会社名、製品名には、各社の商標を含むものもあります。

目次

はじめに

このガイドは、Windows Server 2008 の新機能となるネットワークアクセス保護（NAP）を導入した企業の IT 担当者が、NAP のネットワーク検疫によって出力されるログの収集及び監査を行うための手順を記述するものです。

このガイドを利用することで、企業が定めるネットワーク運用に準拠していることを評価する作業を効率化することを目的としています。

現在、経営/事業における IT の位置づけは、ますます重要度を増しつつあります。

金融商品取引法による財務報告の信頼性を確保するための内部統制や、企業にとって重要な資産である個人情報を漏えいしないための統制など、企業において幅広いコンプライアンスと内部統制環境の構築が求められています。

国内だけではなく、現在のグローバルな経営環境においては、国内の法令や規制だけではなく、ビジネスを展開する様々な国や団体の法令や規制に遵守する必要があります。

現在の経営環境において、企業の内外における IT 環境は、ますます重要度を増しており、またグローバルなビジネスを展開している企業では、ネットワークは世界中に張り巡らされています。こうした環境においては、一つ一つのコンプライアンスの為の IT 基盤を構築するのではなく、将来のコンプライアンスに備えた IT 統制のプロセスと基盤を構築していく必要があります。

適切な IT 統制を行うためには、システム状態を把握するための管理基盤の確立、システムを利用するユーザーのアクセスコントロールは勿論のこと、不正利用などの有事に備えたログの記録及び監査が必要です。

しかしながら、システムの稼働状態やユーザーの操作について、すべてのログを収集し、内容を確認することは、実際の業務を行う上で現実的とは言えません。監査にかかる経費や人手の問題だけでなく、膨大なログのなかに重要な情報が埋もれてしまう危険性も考えられるためです。

そのような事態を回避するためには、本当に必要なログは何であるのか、またどのような手順でどのような点を確認する必要があるのかについて、明確にしておく必要があります。

用語・略語

本書で使用する用語及び略語を、次に示します。

No.	用語・略語	説明
1.	NAP	Networl Access Protection ネットワークアクセス保護
2.	NPS	Network Policy Server ネットワーク ポリシー サーバー
3.	SHV	System Health Validator システム正常性検証ツール
4.	WSHV	Windows System Health Validator Windows セキュリティ正常性検証ツール
5.	SHA	System Health Agent システム正常性エージェント
6.	WSHA	Windows System Health Agent Windows セキュリティ正常性エージェント
7.	NAS	Network Access Server ネットワーク アクセス サーバー
8.	SoH	Statement of Health 正常性ステートメント
9.	TS ゲートウェイ	Terminal Service Gateway ターミナル サービス ゲートウェイ
10.	SQL Server	Microsoft SQL Server 2005

概要

実際の運用において、企業内のネットワークには様々な経路、また大勢のユーザーによってアクセスが行われます。

NAP を利用することにより、企業内ネットワークの運用ポリシーに準拠しないアクセスを検疫することが可能です。それに加えてログの取得及び監査を実施することで、不正利用を抑止し、また有事への対策を強化することができます。

NAP 非 対応のクライアントが多数を占める場合においては、検疫による制限を強制せずに、ネットワークの利用状況や、NAP 対応端末のステータスを確認する目的で NAP および NAP のログ監査を利用することもできます。

本書は、NAP のログ監査を支援するために、必要となる設定及び確認項目を提示します。

NAP について

NAP は、Windows Server 2008 から新しく標準機能として実装されるネットワーク検疫を行う機能です。

NAP で設定した正常性条件に満たないクライアントコンピュータを強制的に隔離されたネットワークへと移動させ、正常性条件を満たす適切な設定がなされるまで、社内 LAN に接続させないようにすることが可能です。また、ファイアウォールが無効になっている場合やセキュリティ更新プログラムが適用されていない場合、設定を強制的に変更したり、セキュリティ更新プログラムを適用させたりすることができます。

クライアントとしては Windows Vista 及び Windows XP SP3 以降から NAP に対応した機能が使用可能となります。

本項では、NAP を構成するコンポーネントについて、記載します。

システム正常性検証ツール（SHV）

SHV は SHA に対応するサーバー コンポーネントです。クライアントが保持するべきシステムの正常性条件が設定され、送られてきた正常性ステートメント（SoH）を確認します。

Windows Server 2008 には標準の SHV として、Windows セキュリティ正常性検証ツール（WSHV）が用意されています。

システム正常性エージェント（SHA）

SHA は SHV に対応するクライアント コンポーネントです。SHA はクライアントのシステム状態を監視し、SHA によって監視される設定が適切に構成されているかを判断します。そして、システムの状態を示す SoH を作成します。

Windows Vista および Windows XP SP3 には標準の SHA として、Windows セキュリティ正常性エージェント (WSHA)が用意されています。

NAP エージェント

SHA によって作成された SoH を、クライアントがアクセスを要求する際、またはシステムの状態が変更された際にネットワーク ポリシー サーバーに送信するクライアント コンポーネントです。

実施クライアント

DHCP、正常性登録機関（IPSec）、802.1X、VPN、TS ゲートウェイの 5 種類の実施ポイントと呼ばれるネットワーク アクセス デバイスとやり取りを行うクライアントコンポーネントです。実施ポイント毎に存在します。また、NAP の検疫の結果によって実施ポイントより提供される IP アドレスや証明書などを受け取ります。

ネットワーク ポリシー サーバー

正常性ポリシーに基づいてクライアントの状態を検証し、接続を許可するか制限するかどうかを判断する役割を担うサーバーです。

実施ポイント

ネットワーク ポリシー サーバーで設定されたネットワーク制限を強制する役割を担うアクセス デバイスです。なお、実施ポイントはネットワーク ポリシー サーバーと同じサーバーに構成することも可能です。

各実施ポイントの種類を、次に示します。

- DHCP

  Windows Server 2008 で構築する DHCP サーバーを用いて、NAP 対応クライアントと、DHCP のアドレス要求・リースのやりとりの中で、クライアントの状態のチェックを行い、検疫結果に応じて、通常のアドレスおよび設定をリースするか、制限されたルーティング情報をセットするかにより、アクセスを制限します。

- 正常性登録機関（IPSec）

  Windows Server 2008 で構築する正常性登録機関と呼ばれる専用の Web サイトを用いて、検疫の結果に応じて証明書を発行します。また別途、証明書の有無により、通信を許可・禁止する IPSec ポリシーを作成することで、検疫結果に応じたアクセス制限を実施します。

- 802.1X

  802.1X 認証付スイッチ等のアクセス デバイスを使用して、クライアントがネットワーク接続時に認証する際にクライアントの状態のチェックを行い、クライアントを検疫結果に応じた VLAN に配置します。

- VPN

  Windows Server 2008 で構築する VPN サーバーを用いて、 クライアントが VPN に接続を試みた際にクライアントの状態のチェックを行い、検疫結果に応じて、フィルタリング ルールを切り替えることで、アクセス制限を実施します。

- TS ゲートウェイ

クライアントが Windows Server 2008 で構築する TS ゲートウェイを介したターミナル接続を試みた際にクライアントの状態のチェックを行い、検疫結果に応じて、接続を許可・禁止します。

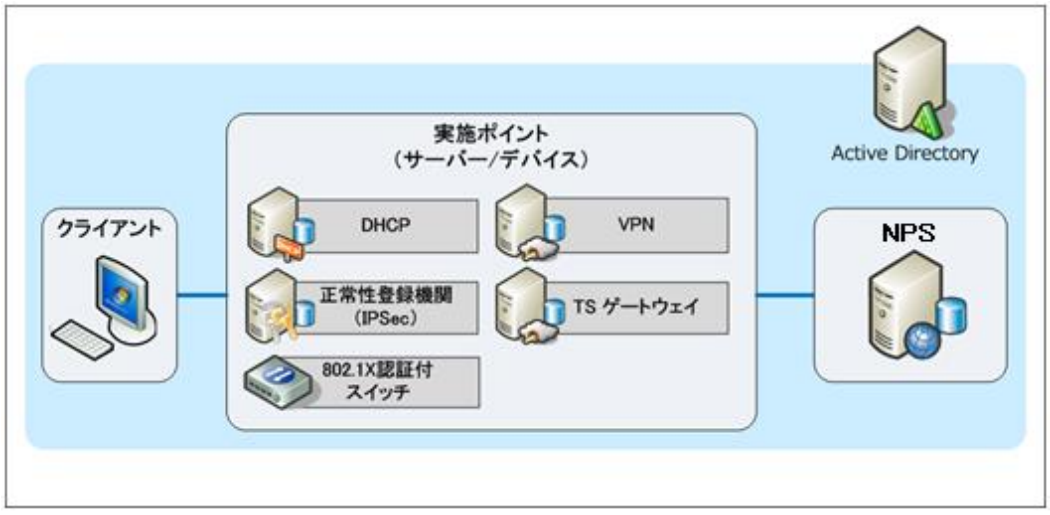
上記の 5 種類のいずれか、または複数組み合わせて利用することが可能です。

環境構成

本書は、監査対象環境の例示として、次の環境を想定して記載します。

Windows Server 2008 のドメイン環境にネットワーク ポリシー サーバーと実施ポイントをそれぞれ別筐体に構成し、ネットワーク ポリシー サーバー、および各実施ポイントにはログ保存用の SQL Server がインストールされていることを想定しています。クライアントはドメインに参加した Windows Vista Enterprise を想定しています。なお、802.1X 認証付スイッチに関するログについては、AlaxalA AX3630 を前提としています。

注意: NAP 機能の利用に当たっては、Windows Server 2008 以前のドメイン環境も利用可能です。また、いくつかの制限はありますが、クライアント端末のドメインへの参加は必須ではありません。下記の図のように、中央の NPS によってポリシーおよびログを一元的に管理する場合には、各実施ポイント側において、ネットワーク ポリシー サーバー機能をインストールし、RADIUS プロキシとして構成します。



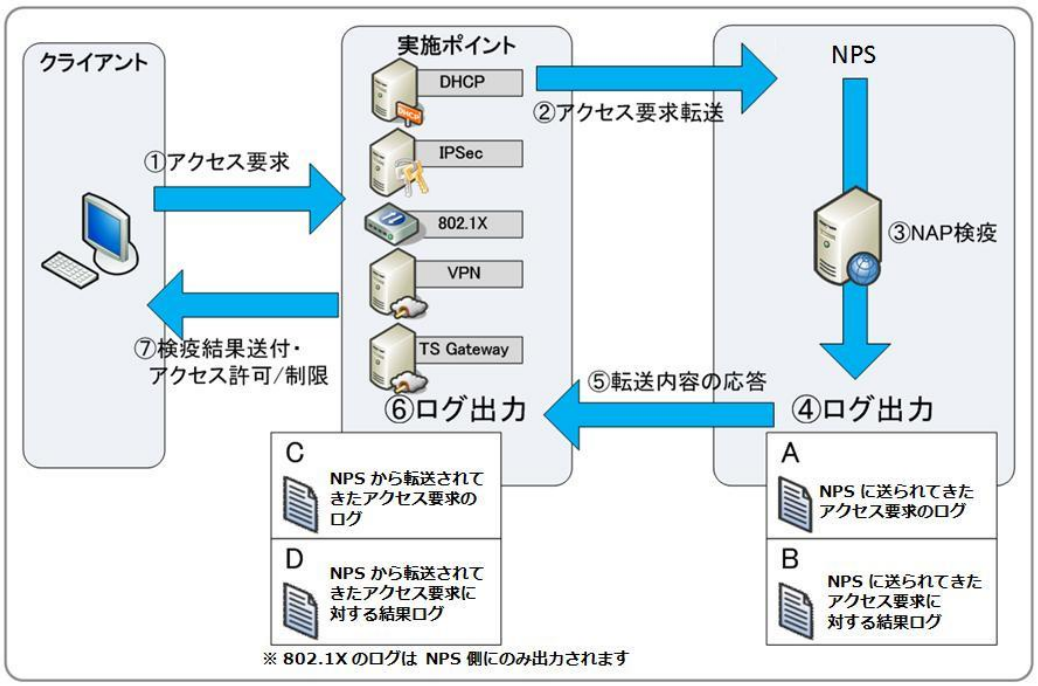
ログの種類及び出力設定

NAP が実施した検疫結果は、NAP 動作時に出力されるログから監査することができます。

本章では、NAP 動作時に出力されるログの種類と、ログの出力設定手順について記述します。

ログの種類と概要

NAP の動作及びログ出力の流れを、次に図示します。



ログの出力設定を行うと、基本的にクライアントのアクセス要求を示す内容のログとクライアントのシステム状態を検証した結果を示すログが 2 件 1 組で出力されます。

また、ネットワーク ポリシー サーバーと実施ポイントを分けて構成した場合、双方で同様のログが出力されますが、ネットワーク ポリシー サーバーのみですべての情報を取得することが可能です。

NAP で取得可能なログの種類は、次の 3 通りです。

- イベント ログ（セキュリティ）
- ローカル ファイル ログ
  - IAS 形式
  - データベース互換形式
- SQL Server ログ

※イベント ログ、ローカル ファイル ログ、SQL Server ログの 3 つ全てを有効にすることが可能です。ただし、ローカル ファイル ログについては、IAS 形式か、データベース互換形式かのいずれかを選択する必要があります。

※802.1X 認証付スイッチ、VPN、TS ゲートウェイを使用した場合、ローカル ファイル ログ、SQL Server ログにはアカウンティング ログを追加で出力することができます。

なお、ローカル ファイル ログ、SQL Server ログは出力するための設定が必要です。設定手順については、P.20「

ログ出力設定」を参照して下さい。

各ログの各形式の詳細について、次に示します。

イベント ログ（セキュリティ）

イベント ログのセキュリティに「ネットワーク ポリシー サーバー」というタスクのカテゴリで、出力されるログです。イベント ビューアから参照する場合には、セキュリティ ログからだけではなく、「カスタム ビュー」、「サーバーの役割」を順に展開し、「ネットワーク ポリシーとアクセス サービス」のビューからも見ることができます。「カスタム ビュー」から参照すると、ネットワーク ポリシー サーバーに関するログだけをフィルタリングして見ることができるので、見やすくなります。イベント ログ（セキュリティ）に出力された NPS イベントの例を、次に示します。

イベント ログ（セキュリティ）の特徴は、次の通りです。

- クライアントの接続試行の結果によって、[成功の監査] か[失敗の監査] が出力されます。
- すべてテキストで記載されているため、最も内容が理解しやすい形式になっています。
- 検疫結果によって、出力されるイベント ID が変化します。
- NPS コンソールでログに記録するよう設定した情報が出力されます。
- NPS でエラーが起こり、NAP の検疫操作が行われなかった場合にも出力されます。

クライアントの接続試行が成功したか失敗したかで次の 2 種類に分かれます。

- アクセス要求成功
  クライアントがフルアクセス、またはネットワーク制限で接続を許可された場合に、[成功の監査] として出力されます。
  クライアントに付与されたアクセス権が、フルアクセスの場合は[ID 6272] /[ID 6276] イベント ログ、ネットワーク制限の場合は[ID 6272] / [ID 6278] イベント ログが出力されます。
- アクセス要求失敗
  クライアントの接続を拒否した場合や NAP に障害が発生した場合などでクライアントが接続失敗した場合に、[失敗の監査] として出力されます。
  NAP のポリシーによって接続を拒否した場合は[ID 6273] イベント ログ、NPS に障害が発生した場合は[ID 6274] イベント ログが出力されます。

NPS イベントの詳細には、クライアント情報、アクセスした実施ポイント、認証の情報、検疫情報などの内容が出力されます。

なお、成功の監査も失敗の監査も既定で出力されるようになっています。成功の監査も記録するようにした場合は、イベント ログのサイズに注意して下さい。

ローカル ファイル ログ IAS 形式

ローカル ファイル ログの IAS 形式では、基本的なヘッダー情報と、追加の属性情報が、カンマ区切りで出力されます。

ローカル ファイル ログ IAS 形式の例を、次に示します。

```
192.168.10.4,,01/17/2008,13:13:40,IAS,NAPNPS,25,311 1 ::1 01/11/2008 07:10:03
182,8153,0,8111,1,44,950450616,6,2,4108,192.168.10.4,4116,0,4128,DHCP_NAPNET,
7,1,8136,0,4154,NAP DHCP,4155,1,8133,{5D2AA831-8E70-4699-BB11-C46158B368E3} -
2008-01-17 04:13:03.106Z,8148,6.0.6000 0.0 x86 ドメイン コントロー
ラ ,8129,NAPLAB\NAPVISTA$,4127,7,8124,Windows セキュリティ正常性検証ツール..:非準
拠 :データなし :なし : (0xc0ff0001 - システム正常性コンポーネントが有効になっていませ
ん。 ..) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0
- ) ,4149,NAP DHCP 非準拠,4136,2,4142,0
```

この形式の特徴は、次の通りです。

- 属性の種類・属性の数は、要求を転送してくる実施ポイントによって異なります。
- ログに記録される属性には、RADIUS 標準、IAS 固有、およびベンダ固有の属性が含まれます。
- 属性が属性 ID という数字で表現されており、また値も特定の内容を意味する数字で記載されているため、内容を理解するためには、属性および属性値 の対応を確認する必要があります。詳細については、P.61「付録 3: 属性と属性値一覧表」を参照してください。
- 最初の 6 個の値は決まった属性で構成されたヘッダーとなっています。ヘッダーの後に続く項目は、属性とその値の組み合わせで出力されます。

最初の 6 項目で構成されるヘッダーの内容は、次の通りです。

例に表示されている値	属性	属性 ID	説明
192.168.10.4	NAS-IP-Address	IAS Header	要求を送信している NAS(実施ポイント) の IP アドレス
（空欄）※	User-Name	IAS Header	アクセスを要求しているユーザーの名前
01/17/2008	Record-Date	IAS Header	ログが書き込まれた日付
13:13:40	Record-Time	IAS Header	ログが書き込まれた時刻
IAS	Service-Name	IAS Header	RADIUS サーバーで実行されているサービスの名前
NAPNPS	Computer-Name	IAS Header	RADIUS サーバーの名前

※ログの例では、User-Name を出力しない DHCP のものであるため、空欄となっています。

ヘッダーの後には、属性とその値とが次のような形式で出力されます。

6 つの属性からなるヘッダー情報 , 属性 ID , 属性値 , 属性 ID , 属性値 , ・・・・

ログの例の「4149,NAP DHCP 非準拠,」部分は、次のように解釈します。

例に表示されている値	説明
4149	属性 **ID 4149** は **NP-Policy-Name** に対応
NAP DHCP 非準拠	適用された ネットワーク ポリシー名

NAP の検疫操作でローカル ファイル ログ IAS 形式に出力される属性については、P.53「付録 2:ローカル ファイル ログ IAS 形式/SQL Server ログ 出力属性一覧」を参照して下さい。

ローカル ファイル ログ データベース互換形式

ローカル ファイル ログ データベース互換形式は、出力されるように設定された NAP の検疫操作情報が、一定の属性の順序に沿って出力されます。

ローカル ファイル ログ データベース互換形式の例を、次に示します。

```
NAPNPS,"IAS",01/17/2008,14:00:07,2,,,,,,,,,0,"192.168.10.4","DHCP NAPNET",,,
,,1,2,7,"NAP DHCP 非準拠",0,"311 1 ::1 01/11/2008 07:10:03
184",,,,,,,,,"4053513845",,,,,,,,,,,,,,,,,,,,,,,,"NAP DHCP",1,,,,
```

この形式の特徴は、次の通りです。

- 要求を転送する実施ポイントに関係なく、一定の属性が同じ順序で出力されます。値が出力されない場合は、空欄となります。
- 属性によっては、値が特定の内容を意味する数字で記載されているため、内容を理解するためには、属性値 ID の対応表を参照する必要があります。詳細については、P.61「付録 3: 属性と属性値一覧表」を参照してください。
- 出力される属性は IAS 形式と比較して非常に少なく、NAP に関する内容が出力される ID 8000 以降が出力されないため、NAP 環境のログ形式としては、適切ではありません。

NAP の検疫操作でローカル ファイル ログ データベース互換形式に出力される属性および出力順については、P.61「付録 3: 属性と属性値一覧表」を参照してください。

SQL Server ログ

SQL Server ログは、NAP の検疫操作情報を、SQL Server に出力するログ形式です。

SQL Server ログには、IAS 形式やデータベース互換形式で出力する内容がすべて含まれています。NAP の検疫操作の監査に使用するには、SQL Server ログを使用することを推奨します。

NPS はログの内容を XML 形式で SQL Server に出力します。出力された XML を受け取るには、”report_event” という決まって名前でのストアド プロシージャを作成し、そのストアド プロシージャを用いて XML 形式のデータを分解し、テーブルにデータを書き込むようにします。

このログの特徴は、次の通りです。

- 属性の種類や順序は、要求を転送してくる実施ポイントの種類によって異なります。
- ログを保存するためのテーブルやストアドプロシージャを作成する必要があります。
- ストアドプロシージャを使って、不必要な属性を記録しないようにしたり、値を加工することが可能です。
- SQL 上のテーブルに格納されたデータを SQL Server Reporting Services 等を利用して、レポートに加工するなどの拡張が容易です。

SQL Server に出力される XML 形式のログの内容を、次に示します。なお、SQL Server Profiler 機能を使うことで、送られてくる内容を直接確認できます。

```
<Event><Computer-Name data type="1">NAPNPS</Computer-Name><Event-Source
data type="1">IAS</Event-Source><Class data type="1">311 1 ::1 01/11/2008
07:10:03 182</Class><MS-Extended-Quarantine-State data_type="0">0</MS-
Extended-Quarantine-State><MS-Quarantine-State data_type="0">1</MS-
Quarantine-State><Acct-Session-Id data_type="1">950450616</Acct-Session-
Id><Service-Type data_type="0">2</Service-Type><Client-IP-Address
data_type="3">192.168.10.4</Client-IP-Address><Client-Vendor
data_type="0">0</Client-Vendor><Client-Friendly-Name
data_type="1">DHCP_NAPNET</Client-Friendly-Name><Framed-Protocol
data type="0">1</Framed-Protocol><Quarantine-Update-Non-Compliant
data_type="0">0</Quarantine-Update-Non-Compliant><Proxy-Policy-Name
data_type="1">NAP DHCP</Proxy-Policy-Name><Provider-Type
data type="0">1</Provider-Type><Quarantine-Session-Id
data_type="1">{5D2AA831-8E70-4699-BB11-C46158B368E3} - 2008-01-17
04:13:03.106Z</Quarantine-Session-Id><Machine-Inventory
data type="1">6.0.6000 0.0 x86 ドメイン コントローラ </Machine-Inventory><Fully-
Qualified-Machine-Name data_type="1">NAPLAB\NAPVISTA$</Fully-Qualified-
Machine-Name><Authentication-Type data_type="0">7</Authentication-
Type><System-Health-Result data type="1">Windows セキュリティ正常性検証ツール..:非
準拠 :データなし :なし : (0xc0ff0001 - システム正常性コンポーネントが有効になっていませ
ん。 ..) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0
- ) </System-Health-Result><NP-Policy-Name data type="1">NAP DHCP 非準拠</NP-
Policy-Name><Packet-Type data_type="0">2</Packet-Type><Reason-Code
data_type="0">0</Reason-Code></Event>
```

<Event>の後には、属性と属性値が次のような形式で出力されます。

```
<属性名 date_type="ログのデータ型">属性値</属性名>
```

SQL Server ログの構成方法については、P.23 「SQL Server ログの構成」を参照してください。NAP の検疫操作で SQL Server ログに出力される属性については、P.53 「付録 2:ローカル ファイル ログ IAS 形式/SQL Server ログ 出力属性一覧」を参照して下さい。

SQL Server ログを長期保存する場合は、データの容量に注意して下さい。

補足: アカウティング ログについて

802.1X、VPN、TS ゲートウェイを利用した場合では、通常の NAP のログに加えてアカウンティング ログをローカル ファイル ログおよび SQL Server ログに記録することができます。

アカウンティング ログとは、接続開始 ・一定期間ごと・接続終了のタイミングで、ログを記録し、接続時間や、送受信パケット量を見るためのものです。

NAP ログのうち、属性 ID 4136 ”Packet-Type” が値 4 “Accounting-Request” となっているものがアカウンティング ログにあたります。なお、アカウンティング ログのうち、属性 ID 40 “ Acct-Status-Type” の、値が 1 であれば “ Start”(接続開始)、2 であれば、” Stop”(接続終了) 、3 であれば” Interim Update”(中間アップデート)を示します。詳細については、P.61「付録 3: 属性と属性値一覧表」を参照してください。

アカウンティング ログの例を、次に示します。

```
192.168.10.254,NAPLAB\napuser,02/07/2008,14:29:56,IAS,NAPNPS,44,000080000027,
40,1,45,1,41,0,5,4296,61,15,87,DVLAN,31,00-11-25-78-22-
62,6,2,4,192.168.10.254,4108,192.168.10.254,4116,0,4128,AX3630S-001,4154,NAP
802.1X スイッチ認証要求,4136,4,4142,0
```

※ローカル ファイルログ IAS 形式

アカウンティング ログからは、次のことが確認できます。
注意: 802.1X 認証機能付スイッチの場合、スイッチの機種や設定により、取得可能な属性が異なる場合があります。

- ユーザー名
- クライアントマシン情報
- 受信オクテット量
- 送信オクテット量
- 接続開始 /切断時刻
- 接続継続時間（秒単位）
- 受信パケット量
- 送信パケット量
- 接続が終了した理由
- RADIUS クライアントの IP アドレス
- RADIUS クライアントのフレンドリ名
- 実施ポイントの種類

上記の情報が確認できる属性を、次に示します。

属性 ID	属性	確認可能項目	802.1X	VPN	TS ゲートウェイ
1	User-Name	ユーザー名	○	○	○
31	Calling-Station-Id	クライアントマシン情報	MAC アドレス	IP アドレス	IP アドレス
42	Acct-Input-Octets	受信オクテット量	○	○	○
43	Acct-Output-Octets	送信オクテット量	○	○	○
44	Acct-Status-Type	接続開始/切断	○	○	○
46	Acct-Session-Time	接続継続時間（秒単位）	○	○	×
47	Acct-Input-Packets	受信パケット量	○	○	×
48	Acct-Output-Packets	送信パケット量	○	○	×
49	Acct-Terminate-Cause	接続が終了した理由	○	○	×
4108	Client-IP-Address	RADIUS クライアントの IP アドレス	○	○	○
4128	Client-Friendly-Name	RADIUS クライアントのフレンドリ名	○	○	○
8132	MS-Network-Access-Server-Type	実施ポイントの種類	○	○	○
8138	MS-Machine-Name	クライアントマシン情報	×	×	IP アドレス

ログ出力設定

NPS のログを出力する方法には、次の 3 種類があります。

- イベント ログ
  イベント ビューアのセキュリティに出力されます。
  クライアントのアクセス要求の成功及び失敗、NPS コンソールで記録するように設定した情報、NPS の障害情報が出力されます。
- ローカル ファイル ログ
  ローカルにテキスト ファイルで保存されるログです。
  ユーザー認証やアカウンティング要求を記録したログが出力されます。
  出力形式には IAS、またはデータベース互換を選択することができます。
- SQL Server ログ
  ローカルの SQL Server に保存されるログです。
  ユーザー認証やアカウンティング要求を記録したログが出力されます。

イベント ログ以外のログを出力するには、設定を行う必要があります。

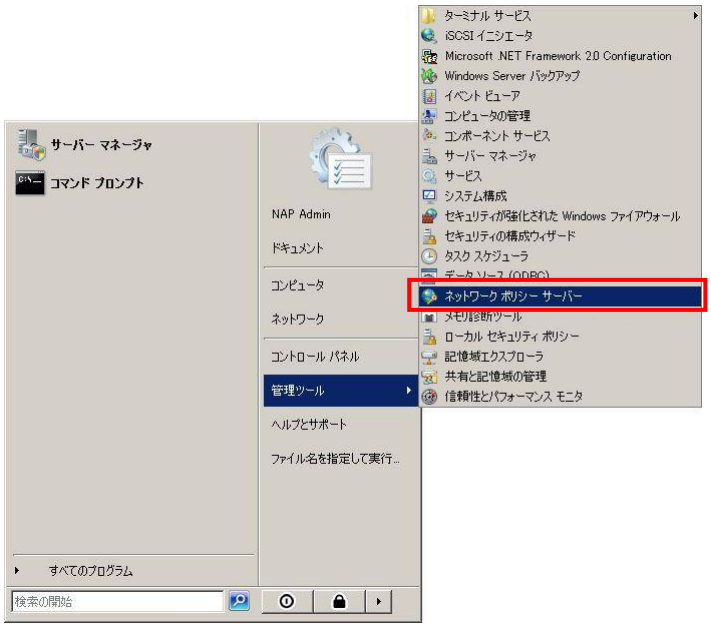
本項では、ローカル ファイル ログと SQL Server ログの出力設定手順を記載します。

ローカル ファイル ログ出力設定

ローカル ファイル ログの出力設定は、NPS コンソールより構成します。

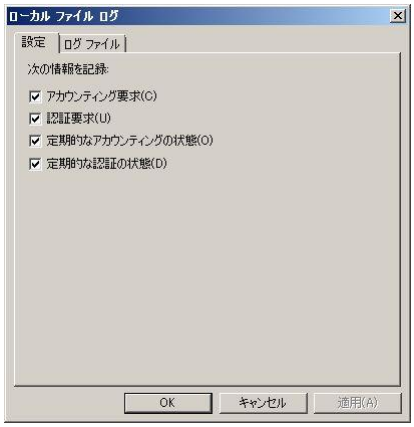
設定手順を、次に示します。

1. 管理者アカウントにて、ログの出力設定を行うネットワーク ポリシー サーバーにログオンします。
2. [スタート]より、[管理ツール]ー[ネットワーク ポリシー サーバー]をクリックします。



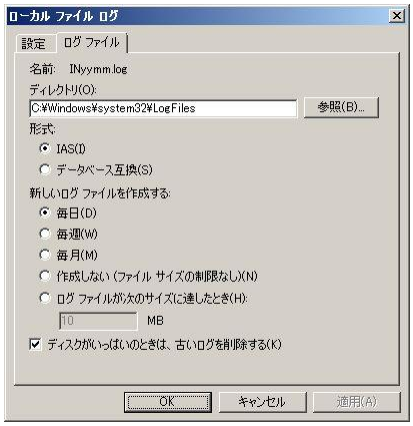
3. [ネットワーク ポリシー サーバー]が開いたら、[アカウンティング]をクリックし、右ペインの[ローカル ファイル ログ] ー[ローカル ファイル ログの構成] をクリックします。

4. [ローカル ファイル ログ] ダイアログ ボックスが表示されたら、[設定]タブにて、ログに記録する情報を選択します。



- アカウンティング要求：すべてのアカウンティング要求を記録します。
- 認証要求：クライアントの認証要求をログに記録します。
- 定期的なアカウンティングの状態：中間報告など定期的な状態を記録します。
- 定期的な認証の状態：中間報告など定期的な状態を記録します。

5. [ログ ファイル] タブをクリックします。



6. [ディレクトリ] に、NPS ログ ファイルの格納先を入力します。
既定の場所は、「C:\Windows\System32\LogFiles 」フォルダです。

7. [形式] にて、ローカル ファイル ログの出力形式を選択します。
既定では、データベース互換の形式が選択されていますが、NAP 固有の属性を含めて記録する場合には、IAS 形式を選択します。

出力形式の詳細については P.14「ローカル ファイル ログ IAS 形式」、P.15「ローカル ファイル ログ データベース互換形式」を参照して下さい。

8. 新しいログを開始する頻度を設定します。
毎日、毎週、毎月、ログが指定したサイズになったときのいずれかに指定できます。
   - 毎日：トランザクション量とログ処理が非常に多い場合に推奨します。
   - 毎週：トランザクション量とログ処理が比較的少ない場合に推奨します。
   - 作成しない（ファイル サイズの制限なし）：1 つのログ ファイルにすべてのトランザクションを格納する場合に指定します。
   - ログ ファイルが次のサイズに達したとき：各ログ ファイルのサイズを制限することができます。既定のサイズは 10 MB です。

9. ディスクの空き容量がなくなった場合に自動的にログ ファイルを削除するように設定する場合は、[ディスクがいっぱいのときは、古いログを削除する] をチェックします。
なお、最も古いログ ファイルが現在のログ ファイルの場合は削除されません。

10. [OK] をクリックします。

以上で、ローカル ファイル ログの出力設定は終了となります。

SQL Server ログ出力設定

SQL Server ログを出力するには、次の手順が必要です。

I. XML を取り込むデータベース及びテーブルの作成
II. ログインの作成
III. SQL Server ログの構成

各手順を、次に記述します。

I. XML を取り込むデータベース及びテーブルの作成
XML を取り込むデータベース及びテーブルの作成手順について、次に示します。
   1. 管理者アカウントにて、SQL Server ログを格納する SQL Server にログオンします。
   2. [SQL Server Management Studio]を右クリックし、[管理者として実行]をクリックします。

3. [Microsoft SQL Server Management Studio]が表示されたら、新しいクエリを選択します。
4. P.39「付録 3:SQL Server ログ XML 取り込みストアド プロシージャおよびテーブル」の記載内容に従って、「データベース およびテーブルの作成サンプル SQL 文」および「ストアドプロシージャの作成 サンプル SQL 文」をそれぞれコピー ペーストして、クエリを実行します。

以上で、XML を取り込むデータベース及びテーブルの作成手順は完了となります。

II. ログインの作成

1. 管理者権限のあるユーザーで NAP 管理サーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。

2. [Microsoft SQL Server Management Studio] が起動します。
オブジェクト エクスプローラから、[<*ツリールート*>] - [セキュリティ] - [ログイン] を選択します。右クリックをして、[新しいログイン] を選択します。
3. [ログイン - 新規作成] が表示されます。
[ログイン名] に、NPS の接続で利用するユーザー名を指定します。
[Windows 認証] が選択されていることを確認し、 [既定のデータベース] のドロップダウンリストから、「XML を取り込むデータベース及びテーブルの作成」で作成した[IASODBC] を指定します。

プロパティ名	設定値
ログイン名	***<NPS の接続で利用するユーザー名>***
Windows 認証	○
SQL Server 認証	● （チェック)
パスワード	***<パスワード>***
パスワードの確認入力	***<パスワード>***
パスワードポリシーを適用する	■（グレーアウト）
パスワードの期限を適用する	■（グレーアウト）
ユーザーは次回ログイン時にパスワードを変更する	■（グレーアウト）
証明書にマップ済み	○
証明書名	-（グレーアウト）
非対称キーにマップ済み	-（グレーアウト）
キー名	-（グレーアウト）
既定のデータベース	**IASODBC**

プロパティ名	設定値
既定の言語	既定

4. 画面左の[ページの選択] より、[ユーザー マッピング] をクリックします。
[このログインにマッピングされたユーザー] 欄の[IASODBC] にチェックを入れます。続いて、[IASODBC のデータベース ロール メンバシップ] 欄で、[db_ower] 、[public] にチェックを入れます。
設定が完了したら、[OK] をクリックします。

プロパティ名	設定値	
このログインにマップされたユーザー	-	-
master	☐	-
model	☐	-
msdb	☐	-
tempdb	☐	-
IASODBC	■	*<NAP レポートサーバー用 SQLSERVERAGENT サービス実行ユーザー>*
IASODBC のデータベース ロール メンバシップ	-	
db_accessadmin	☐	
db_backupoperator	☐	
db_datareader	☐	
db_datawriter	☐	
db_ddladmin	☐	
db_denydatareader	☐	
db_denydatawriter	☐	
db_owner	■	
db_securityadmin	☐	
public	■	

5. [Microsoft SQL Server Management Studio] に戻ります。
オブジェクト エクスプローラから、[*<ツリールート>*] - [セキュリティ] - [ログイン] を展開します。展開された一覧に、設定したユーザーが表示されることを確認します。

以上で、ログインの作成は完了となります。

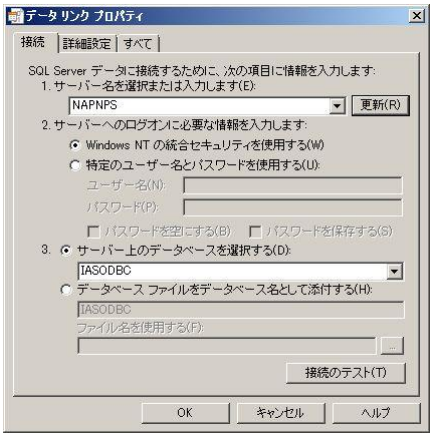
III. SQL Server ログの構成
続いて、SQL Server ログの構成手順について、次に示します。

1. 管理者アカウントにて、SQL Server ログを格納する SQL Server にログオンします。
2. [スタート]より、[管理ツール]−[ネットワーク ポリシー サーバー]をクリックします。
3. [ネットワーク ポリシー サーバー]が開いたら、[アカウンティング]をクリックし、右ペインの[SQL Server ログ]−[SQL Server ログの構成] をクリックします。

4. [SQL Server ログ] ダイアログ ボックスが表示されます。

5. [次の情報を記録] でログに記録する情報を選択します。
   - アカウンティング要求：すべてのアカウンティング要求を記録します。
   - 認証要求：クライアントの認証要求をログに記録します。
   - 定期的なアカウンティングの状態：中間報告など定期的な状態を記録します。
   - 定期的な認証の状態：中間報告など定期的な状態を記録します。

6. NPS を実行するサーバーと SQL Server データベース間の同時セッション数を構成するには、[同時セッションの最大数] に数値を入力します。
7. SQL Server データ ソースを構成するため、[構成] をクリックします。
8. [データ リンクのプロパティ] ダイアログ ボックスの[接続] タブが表示されます。



9. [1. サーバー名を選択または入力します] にて、SQL Server ログを格納する SQL Server のサーバー名を入力し、[更新] をクリックします。
10. [2. サーバーへのログオンに必要な情報を入力します] にて、サーバーへのログオンに使用する認証方法を指定します。
11. [3. サーバー上のデータベースを選択する] にて、SQL Server ログを格納するデータベースを指定します。 ドロップダウンリストに選択可能な一覧が表示されます。
12. NPS を実行するサーバーと SQL Server を実行するコンピュータ間の接続をテストするため、[接続テスト] をクリックします。
13. SQL Server との接続が確認できたら、[OK]をクリックします。

以上で、SQL Server ログの構成は終了となります。

ログの監査手順

本章では、検疫操作によるログの監査を行うために必要となる手順について記述します。

イベント ログの確認

本項では、イベント ログの確認手順について記載します。

イベントログには、「ネットワーク ポリシー サーバー」というタスクのカテゴリで出力され、検疫結果によって出力されるイベント ID が変化します。

検疫結果と出力されるイベント ログの組み合わせを、次に示します。

検疫結果	出力イベント **ID**	説明	備考
フルアクセス	**[ID 6272]**	アクセスを許可	
	[ID 6278]	検疫の結果として フルアクセスを許可	
ネットワーク制限	**[ID 6272]**	アクセスを許可	
	[ID 6276]	検疫の結果として ネットワーク アクセスを制限	
接続を拒否	**[ID 6273]**	アクセスを拒否	
アクセス要求を破棄	**[ID 6274]**	**RADIUS** サーバーが応答しないため、**NPS** がクライアントの要求を破棄	実施ポイントのみで出力。

各イベントログの確認方法を次に示します。

なお、イベントを構成する詳細内容については、P.70「付録 4:イベント ログ（セキュリティ） 一覧」を参照して下さい。

[ID 6272] イベント ログの確認

[ID 6272] イベント ログは NPS がクライアントのアクセス要求を許可したことを示すログです。

[ID 6272] イベントログより確認できる情報は、次の通りです。

- 検疫結果
  ログの詳細欄にある、[検疫情報]－[結果] から確認することができます。
- クライアント情報
  NAP の検疫を受けたユーザー情報は、ログの詳細欄にある[ユーザー]及び[クライアント コンピュータ]から確認することができます。

- アクセス要求を受け取った実施ポイント情報
  ログの詳細欄にある[NAS]から確認することができます。
- 適合したネットワーク ポリシー
  アクセス要求を受け取ったクライアントの条件に適合するネットワーク ポリシーはログの詳細欄にある [認証の詳細] から確認することができます。

[ID 6272] イベント ログには、NAP の検疫結果の原因は含まれません。NAP の検疫結果を監査するには、[ID 6272] イベント ログと紐づく[ID 6276]、または[ID 6278] イベント ログを特定する必要があります。

そのために使用するのが、[認証の詳細]－[アカウントのセッション ID]です。[アカウントのセッション ID]は、サーバーでセッションが行われた際に出力される ID です。

ただし、[アカウントのセッション ID]は、再利用される可能性があります。

そのため、[アカウントのセッション ID]が同一の[ID 6276]、または[ID 6278] イベント ログを特定する場合には、[ID 6276]、または[ID 6278] イベント ログが出力された日時と、最も近い日時に出力されたイベント ログであることを、併せて確認する必要があります。

[ID 6273] イベント ログの確認

[ID 6273] イベント ログは NPS がクライアントのアクセス要求を拒否したことを示すログです。NAP のポリシーによって拒否された場合に出力されます。

[ID 6273] イベントログより確認できる情報は、次の通りです。

- アクセス要求を拒否された理由
  ログの詳細欄にある、[認証の詳細]－[理由] から確認することができます。
- クライアント情報
  アクセス要求を送ったユーザー情報は、ログの詳細欄にある[ユーザー]及び[クライアント コンピュータ]から確認することができます。
- アクセス要求を受け取った実施ポイント情報
  ログの詳細欄にある[NAS]から確認することができます。
- 適合したネットワーク ポリシー
  アクセス要求を受け取ったクライアントの条件に適合するネットワーク ポリシーはログの詳細欄にある [認証の詳細] から確認することができます。

[ID 6274] イベント ログの確認

[ID 6274] イベント ログは RADIUS サーバーが応答しなかったため、クライアントのアクセス要求が破棄されたことを示すログです。実施ポイントに出力されます。

[ID 6274] イベントログより確認できる情報は、次の通りです。

- アクセス要求を拒否された理由
  ログの詳細欄にある、[認証の詳細]－[理由] から確認することができます。
- クライアント情報
  アクセス要求を送ったユーザー情報は、ログの詳細欄にある[ユーザー]及び[クライアント コンピュータ]から確認することができます。

[ID 6276] イベント ログの確認

[ID 6276] イベント ログは NPS がクライアントを検疫したことを示すログです。

[ID 6276] イベントログより確認できる情報は、次の通りです。

- 検疫結果
  ログの詳細欄にある、[検疫情報]－[結果] から確認することができます。
- 検疫された原因
  ログの詳細欄にある、[検疫情報]－[システム正常性検証ツールの結果] から確認することができます。
- クライアント情報
  アクセス要求を送ったユーザー情報は、ログの詳細欄にある[ユーザー]及び[クライアント コンピュータ]から確認することができます。
- アクセス要求を受け取った実施ポイント情報
  ログの詳細欄にある[NAS]から確認することができます。
- 適合したネットワーク ポリシー
  アクセス要求を受け取ったクライアントの条件に適合するネットワーク ポリシーはログの詳細欄にある [認証の詳細] から確認することができます。

[ID 6278] イベント ログの確認

[ID 6278] イベント ログは NPS がクライアントにフル アクセスを許可したことを示すログです。

[ID 6278] イベントログより確認できる情報は、次の通りです。

- 検疫結果
  ログの詳細欄にある、[検疫情報]－[結果] から確認することができます。
- 検疫された原因
  ログの詳細欄にある、[検疫情報]－[システム正常性検証ツールの結果] から確認することができます。
- クライアント情報
  アクセス要求を送ったユーザー情報は、ログの詳細欄にある[ユーザー]及び[クライアント コンピュータ]から確認することができます。
- アクセス要求を受け取った実施ポイント情報
  ログの詳細欄にある[NAS]から確認することができます。

- 適合したネットワーク ポリシー
  アクセス要求を受け取ったクライアントの条件に適合するネットワーク ポリシーはログの詳細欄にある [認証の詳細] から確認することができます。

NPS ログの確認

本項では、テキスト ファイル ログおよび SQL Server ログから確認できる情報を記載します。

検疫結果の確認

NAP によってアクセスを制限、または拒否されたログの監査を行うにはまず、検疫結果が出力された属性から特定を行います。

検疫によってクライアントに実施された結果が確認できる属性は、次の通りです。

属性 ID	属性	属性値 ID	属性値	説明
4136	Packet-Type	1	Access-Request	クライアントの接続要求
		2	Access-Accept	クライアントの接続を許可
		3	Access-Reject	クライアントの接続を拒否
		4	Accounting-Request	アカウンティング要求
		5	Accounting-Response	アカウンティングの応答
		11	Access-Challenge	認証情報の確認
		12	Status-Server（experimental）	
		13	Status-Client（experimental）	
		255	Reserved	
8111	MS-Quarantine-State	0	Full Access	クライアントにフル アクセスを許可
		1	Quarantine	クライアントにネットワーク制限ありでアクセスを許可
		2	Probation	制限対象であるが、特定の日時まではフル アクセスを許可

検疫された原因の確認

検疫された原因は、属性 ID 8124 System Health Result の値から確認することができます。(イベント ログ[ID 6276]、または[ID 6278] に記載されるシステム正常性検証ツールの結果も同じ見方が可能です。)

属性 ID 8124 System Health Result の値は、次の形式で出力されます。

```
Windows セキュリティ正常性検証ツール..:非準拠 :データなし :なし : (0xc0ff0001 - システム正常性コンポーネントが有効になっていません。 ..) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - ) : (0x0 - )
```

値の先頭から、検疫に使用された　SHV 名、準拠・非準拠の結果、詳細情報が確認できます。

「0x0 」は、左から順にそれぞれ SHV の設定項目を意味します。

本項では Windows 正常性検証ツールについて記載します。

WSHV の場合、各項目に当てはまる設定は次の通りです。

項目	設定値
第 1 項目	ファイアウォールの状態
第 2 項目	ウイルス対策ソフトウェアの状態
第 3 項目	ウイルス対策ソフトウェアの定義の状態
第 4 項目	スパイウェア対策ソフトウェアの状態
第 5 項目	スパイウェア対策ソフトウェアの定義ファイルの状態
第 6 項目	自動更新の状態
第 7 項目	セキュリティ更新プログラムの適用状態
第 8 項目	WSHV で設定したセキュリティ更新プログラムのレベル

> 参考：**Windows XP** の **WSHV** 項目
>
> Windows XP の WSHV では次の項目を設定することができません。
>
> ・スパイウェア対策ソフトウェアの状態
>
> ・スパイウェア対策ソフトウェアの定義ファイルの状態
>
> ID 8124 System Health Result は、次のように出力されます。
>
> 第 1 項目：ファイアウォールの状態
>
> 第 2 項目：ウイルス対策ソフトウェアの状態
>
> 第 3 項目：ウイルス対策ソフトウェアの定義の状態
>
> 第 4 項目：自動更新の状態
>
> 第 5 項目：セキュリティ更新プログラムの適用状態
>
> 第 6 項目：WSHV で設定したセキュリティ更新プログラムのレベル

それぞれの項目について、チェックをパスした場合は「0x0 」となり、チェックをパスしなかった場合、各項目に「0x0 」以外の値が出力されます。値は原因によって異なります。

各項目に出力される値の一例を、次に示します。

値
（**0xc0ff0001** - システム正常性コンポーネントが有効になっていません。 **..**）
（**0xc0ff0004** - 特定のシステム正常性コンポーネントの署名が最新ではありません。**..**）：
（**0xc0ff0007** - このコンピュータは **Windows Server Update Services** サーバーと自動的に同期されます。新しいセキュリティ更新プログラムがインストールされる必要があります。**..**）
（**0xc0ff0047** - サードパーティ製のシステム正常性コンポーネントが有効になっていません。 **..**）：
（**0xc0ff000c** - このコンピュータ上の **Windows Update** エージェントは **Windows Server Update Services** サーバーと同期するように構成されていません。管理者が **Windows Update** エージェント サービスを構成する必要があります。構成が完了したら **[**再試行**]** ボタンをクリックして、変更を有効にしてください。**..**）

参考：複数 **SHV** 使用時の出力

SHV を複数設定している場合、ログには設定した数の SHV の結果が複数の 8124 System Health Result として連続して出力されます。
ローカル ファイル ログ IAS 形式 出力例

8124,Windows セキュリティ正常性検証ツール..:準拠 :データなし :なし :(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -),8124,SDK SHV Sample:準拠 :データなし :なし :(0x0 -),

SQL Server ログ出力例

<System-Health-Result data_type="1">Windows セキュリティ正常性検証ツール..:準拠 :データなし :なし :(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -):(0x0 -)</System-Health-Result><System-Health-Result data_type="1">SDK SHV Sample:準拠 :データなし :なし :(0x0 -)</System-Health-Result>

クライアント情報の確認

NPS ログから、ユーザー、またはクライアントマシンを特定することが可能です。

NPS ログで確認できるクライアント情報は、次の通りです。

- ユーザー名
- クライアントマシン情報

上記の情報が確認できる属性を、次に示します。

属性 ID	属性	確認可能項目	備考
1	User-Name	ユーザー名	ユーザー認証をする実施ポイントの場合のみ出力される。
31	Calling-Station-Id	クライアントマシン情報	実施ポイントの種類により、IP アドレスもしくは Mac アドレスで出力される。
4129	SAM-Account-Name	ユーザー名	ユーザー認証をする実施ポイントの場合のみ、ネットワーク ポリシー サーバー上で出力される。
4130	Fully-Qualifed-User-Name	ユーザー名	ユーザー認証をする実施ポイントの場合のみ出力される。
8129	Fully-Qualified-Machine-Name	クライアントマシン情報	ドメイン参加時にのみ出力される。
8138	MS-Machine-Name	クライアントマシン情報	

なお、ユーザー名、クライアントマシン情報は、実施ポイントの種類、クライアントが NAP 対応か非対応か、ドメインに参加しているかなどで、属性値の出力の有無や出力形式が異なります。差異を、次に一覧で示します。

凡例：○…確認可能、×…確認不可能、－…NAP によるログ出力なし

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X		VPN		TS ゲートウェイ	
		NAP 対応	NAP 非対応	NAP 対応	NAP 非対応	NAP 対応	NAP 非対応	NAP 対応	NAP 非対応	NAP 対応	NAP 非対応
1	User-Name	×	×	×	－	○ ユーザー名 or マシン名	○ ユーザー名 or マシン名	○ ユーザー名	○ ユーザー名	○ ユーザー名	○ ユーザー名
31	Calling-Station-Id	○ Mac アドレス	○ Mac アドレス	×	－	○ Mac アドレス	○ Mac アドレス	○ IP アドレス	○ IP アドレス	×	×
4129	SAM-Account-Name	×	×	×	－	○ ユーザー名 or マシン名	○ ユーザー名 or マシン名	○ ユーザー名	○ ユーザー名	○ ユーザー名	○ ユーザー名
4130	Fully-Qualifed-User-Name	×	×	×	－	○ ユーザー名 or マシン名	○ ユーザー名 or マシン名	○ ユーザー名	○ ユーザー名	○ ユーザー名	○ ユーザー名
8129	Fully-Qualified-Machine-Name	○ ドメイン参加時	×	○ ドメイン参加時	－	○ ドメイン参加時	×	○ ドメイン参加時	×	○ ドメイン参加時	×
8138	MS-Machine-Name	○	○	×	－	○ ドメイン参加時	×	×	×	○	○

適用された NAP 設定の確認

NPS ログから、NAP で設定した内容を確認することが可能です。

NPS ログで確認できる NAP の設定項目は、次の通りです。

- RADIUS クライアント(実施ポイント)のフレンドリ名
- 適用されたネットワークポリシー名
- 適用されて接続要求ポリシー名
- 実施ポイントの種類

上記の情報が確認できる属性を、次に示します。

属性 ID	属性	確認可能 NAP 設定項目	備考
4128	Client-Friendly-Name	RADIUS クライアント名 のフレンドリ名	実施ポイントと、ネットワーク ポリシー サーバーを分けた場合、RADIUS プロキシのために設定した RADIUS クライアントの名前が記録されます。
4149	NP-Policy-Name	ネットワーク ポリシー名	適用されたネットワーク ポリシー名が記録されます。
4154	Proxy-Policy-Name	接続要求ポリシー名	適用された接続要求ポリシー名が記録されます。
8132	MS-Network-Access-Server-Type	実施ポイントの種類	出力される値は、次の通り。 · 0 = 指定なし · 1 =ターミナル サーバー ゲートウェイ · 2 =リモート アクセス サーバー (VPN - ダイヤルアップ) · 3 = DHCP サーバー · 5 =正常性登録機関 · 6 = HCAP サーバー

おわりに

以上の各章にて、NAP の検疫操作におけるログについて、出力に必要な設定及び監査可能な要素を記載してきました。

IT 統制における監査は、必ずしも専用のソリューション製品の導入や専門機関への委託なしに実現不可能なものではありません。

また、無作為なログの収集は、結果的に監査に必要となるコスト、時間、人員を増大させるのみならず、監査結果の信頼性を低める事態にも繋がる可能性があります。

適切かつ有効な監査を実施するためには、まず監査すべき情報や手順を明確化することが重要です。

監査対象とする要素の性質を把握し、それに見合った監査を検討されるにあたり、本書がその手助けとなりましたら幸いです。

付録1: SQL Server ログ XML 取り込みストアド プロシージャおよびテーブル

本書で使用した NPS から送信された XML をテーブルに取り込むためのストアド プロシージャおよびテーブルを作成するための SQL 文を、次に記載します。

データベースおよびテーブルの作成サンプル SQL 文

```
IF EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE name =
N'IASODBC')
    DROP DATABASE [IASODBC]
GO

DECLARE @DataPath nvarchar(255)
DECLARE @LogPath nvarchar(255)

/***********************************/
/** DB ファイルの保存先を変更する場合は、以下の DataPath、LogPath に指定されているパスを変更してください。**/
/** ファイルの保存先には、ファイルの書き込み権限が必要となります。 **/
/***********************************/
Select @DataPath = 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\'
Select @LogPath = 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\'

If @DataPath = ''
    Select @DataPath = 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\'
Else If Right(@DataPath,1) <> '\'
    Select @DataPath = @DataPath + '\'

If @LogPath = ''
    Select @LogPath = 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\'
Else If Right(@LogPath,1) <> '\'
    Select @LogPath = @LogPath + '\'

Select @DataPath = @DataPath + 'IASODBC_Data.MDF'
Select @LogPath = @LogPath + 'IASODBC_Log.LDF'

EXECUTE ('CREATE DATABASE [IASODBC] ON
( NAME = IASODBC_Data, FILENAME = ''' + @DataPath + ''' , SIZE =
10240KB , MAXSIZE = UNLIMITED, FILEGROWTH = 10% )
 LOG ON
( NAME = IASODBC_Log, FILENAME = ''' + @LogPath +  ''' , SIZE =
10240KB , MAXSIZE = UNLIMITED , FILEGROWTH = 10%)
```

```
 COLLATE SQL_Latin1_General_CP1_CI_AS')
GO

exec sp_dboption N'IASODBC', N'autoclose', N'false'
GO

exec sp_dboption N'IASODBC', N'bulkcopy', N'false'
GO

exec sp_dboption N'IASODBC', N'trunc. log', N'false'
GO

exec sp_dboption N'IASODBC', N'torn page detection', N'true'
GO

exec sp_dboption N'IASODBC', N'read only', N'false'
GO

exec sp_dboption N'IASODBC', N'dbo use', N'false'
GO

exec sp dboption N'IASODBC', N'single', N'false'
GO

exec sp dboption N'IASODBC', N'autoshrink', N'false'
GO

exec sp dboption N'IASODBC', N'ANSI null default', N'false'
GO

exec sp dboption N'IASODBC', N'recursive triggers', N'false'
GO

exec sp dboption N'IASODBC', N'ANSI nulls', N'false'
GO

exec sp dboption N'IASODBC', N'concat null yields null', N'false'
GO

exec sp dboption N'IASODBC', N'cursor close on commit', N'false'
GO

exec sp dboption N'IASODBC', N'default to local cursor', N'false'
GO

exec sp dboption N'IASODBC', N'quoted identifier', N'false'
GO

exec sp dboption N'IASODBC', N'ANSI warnings', N'false'
GO

exec sp dboption N'IASODBC', N'auto create statistics', N'true'
GO
```

```
exec sp_dboption N'IASODBC', N'auto update statistics', N'true'
GO

if( ( (@@microsoftversion / power(2, 24) = 8) and (@@microsoftversion
& 0xffff >= 724) ) or ( (@@microsoftversion / power(2, 24) = 7) and
(@@microsoftversion & 0xffff >= 1082) ) )
    exec sp_dboption N'IASODBC', N'db chaining', N'false'
GO

USE [IASODBC]
GO
/****** オブジェクト:  UserDefinedDataType [dbo].[ipaddress]    スクリプ
ト日付: 03/18/2008 19:06:30 ******/
CREATE TYPE [dbo].[ipaddress] FROM [nvarchar](15) NOT NULL
GO
/****** オブジェクト:  Table [dbo].[NAP_TransportLog_Table]    スクリプト
日付: 03/18/2008 19:06:30 ******/
SET ANSI_NULLS ON
GO
SET QUOTED IDENTIFIER ON
GO

/****** オブジェクト:  Table [dbo].[accounting data]    スクリプト日付:
03/18/2008 19:06:31 ******/
SET ANSI NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[accounting_data](
    [id] [int] IDENTITY(1,1) NOT NULL,
    [timestamp] [datetime] NOT NULL,
    [Computer_Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL,
    [Event Source] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS_MPPE_Encryption_Types] [int] NULL,
    [MS Link Drop Time Limit] [int] NULL,
    [MS_Link_Utilization_Threshold] [int] NULL,
    [User_Name] [nvarchar](255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL,
    [NAS_IP_Address] [dbo].[ipaddress] NULL,
    [NAS_Port] [int] NULL,
    [Service Type] [int] NULL,
    [Framed_Protocol] [int] NULL,
    [Framed_IP_Address] [dbo].[ipaddress] NULL,
    [Framed MTU] [int] NULL,
    [Class] [nvarchar](255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL,
    [Vendor Specific] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Called_Station_Id] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Calling_Station_Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
```

```
    [NAS_Identifier] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Acct Status Type] [int] NULL,
    [Acct_Delay_Time] [int] NULL,
    [Acct_Input_Octets] [int] NULL,
    [Acct_Output_Octets] [int] NULL,
    [Acct_Session_Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Acct_Authentic] [int] NULL,
    [Acct_Session_Time] [int] NULL,
    [Acct_Input_Packets] [int] NULL,
    [Acct_Output_Packets] [int] NULL,
    [Acct_Terminate_Cause] [int] NULL,
    [Acct Multi Session Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Acct_Link_Count] [int] NULL,
    [Event Timestamp] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [NAS_Port_Type] [int] NULL,
    [Tunnel Type] [int] NULL,
    [Tunnel_Medium_Type] [int] NULL,
    [Tunnel Client Endpt] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Connect_Info] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Tunnel Pvt Group Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Acct Interim Interval] [int] NULL,
    [NAS_Port_Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Client IP Address] [dbo].[ipaddress] NULL,
    [Client_Vendor] [int] NULL,
    [MS_CHAP_Domain] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Authentication_Type] [int] NULL,
    [Client_Friendly_Name] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [SAM_Account_Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Fully Qualifed User Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [EAP_Friendly_Name] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Packet_Type] [int] NOT NULL,
    [Reason_Code] [int] NULL,
    [MS RAS Vendor] [int] NULL,
    [MS_RAS_Version] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [NP Policy Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Proxy_Policy_Name] [nvarchar](255) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Provider_Type] [int] NULL,
```

```
    [Provider_Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Remote Server Address] [dbo].[ipaddress] NULL,
    [MS_RAS_Client_Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS_RAS_Client_Version] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS_PEAP_Fast_Roamed_Session] [int] NULL,
    [MS_Identity_Type] [int] NULL,
    [MS_Service_Class] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS_Quarantine_State] [int] NULL,
    [System_Health_Result_1] [nvarchar](4000) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [System_Health_Result_2] [nvarchar](4000) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [System Health Result 3] [nvarchar](4000) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [System_Health_Result_4] [nvarchar](4000) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [System_Health_Result_5] [nvarchar](4000) COLLATE
SQL Latin1 General CP1 CI AS NULL,
    [Fully Qualified Machine Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS Network Access Server Type] [int] NULL,
    [Quarantine Session Id] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Quarantine Update Non Compliant] [int] NULL,
    [MS_Machine_Name] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [Machine Inventory] [nvarchar](255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL,
    [MS_Extended_Quarantine_State] [int] NULL,
    [DB XML] [nvarchar](max) COLLATE SQL Latin1 General CP1 CI AS
NULL
) ON [PRIMARY]
GO
```

XML 取り込む際に、利用するストアドプロシージャを作成するための SQL 文を、次に記載します。属性 ID 8124 System Health Result の値の並び替えを行うためのストアドプロシージャも合わせて作成します。

ストアドプロシージャの作成 サンプル SQL 文

```
USE IASODBC
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
-- ============================================
-- Create date: 2008/03/07
-- Description:    SHR を、対応する列に格納するために、並び替える。
-- Input:          @tool_name nvarchar(255)      : ツール名
```

```
--                          @tool_number int       : ツールの結果を格納する
列番号
--                          @str1 nvarchar(max)    : SHR1 個目の出力内容
--                          @str2 nvarchar(max)    : SHR2 個目の出力内容
--                          @str3 nvarchar(max)    : SHR3 個目の出力内容
--                          @str4 nvarchar(max)    : SHR4 個目の出力内容
--                          @str5 nvarchar(max)    : SHR5 個目の出力内容
-- ============================================
CREATE PROCEDURE [dbo].[Sort_SHR]
(
    @tool_name nvarchar(255) ,
    @tool_number int ,
    @str1 nvarchar(max)    OUTPUT ,
    @str2 nvarchar(max)    OUTPUT ,
    @str3 nvarchar(max)    OUTPUT ,
    @str4 nvarchar(max)    OUTPUT ,
    @str5 nvarchar(max)    OUTPUT
)
AS
BEGIN

    SET NOCOUNT ON;

    DECLARE @str6 nvarchar(max)
    DECLARE @number int

    Set @number = 0

    If CharIndex(@tool_name,@str1) = 1
    Begin
            If @tool number = 2
            Begin
                    Set @str6 = @str1
                    Set @str1 = @str2
                    Set @str2 = @str6
            End
            If @tool number = 3
            Begin
                    Set @str6 = @str1
                    Set @str1 = @str3
                    Set @str3 = @str6
            End
            If @tool number = 4
            Begin
                    Set @str6 = @str1
                    Set @str1 = @str4
                    Set @str4 = @str6
            End
            If @tool number = 5
            Begin
                    Set @str6 = @str1
                    Set @str1 = @str5
                    Set @str5 = @str6
            End
```

```
        Set @number = 1

End

If CharIndex(@tool_name,@str2) = 1
Begin
        If @tool_number = 1
        Begin
                Set @str6 = @str2
                Set @str2 = @str1
                Set @str1 = @str6
        End
        If @tool number = 3
        Begin
                Set @str6 = @str2
                Set @str2 = @str3
                Set @str3 = @str6
        End
        If @tool number = 4
        Begin
                Set @str6 = @str2
                Set @str2 = @str4
                Set @str4 = @str6
        End
        If @tool number = 5
        Begin
                Set @str6 = @str2
                Set @str2 = @str5
                Set @str5 = @str6
        End

        Set @number = 2

End

If CharIndex(@tool name,@str3) = 1
Begin
        If @tool_number = 1
        Begin
                Set @str6 = @str3
                Set @str3 = @str1
                Set @str1 = @str6
        End
        If @tool_number = 2
        Begin
                Set @str6 = @str3
                Set @str3 = @str2
                Set @str2 = @str6
        End
        If @tool_number = 4
        Begin
                Set @str6 = @str3
                Set @str3 = @str4
```

```
                Set @str4 = @str6
        End
        If @tool number = 5
        Begin
                Set @str6 = @str3
                Set @str3 = @str5
                Set @str5 = @str6
        End

        Set @number = 3

End

If CharIndex(@tool name,@str4) = 1
Begin
        If @tool_number = 1
        Begin
                Set @str6 = @str4
                Set @str4 = @str1
                Set @str1 = @str6
        End
        If @tool number = 2
        Begin
                Set @str6 = @str4
                Set @str4 = @str2
                Set @str2 = @str6
        End
        If @tool number = 3
        Begin
                Set @str6 = @str4
                Set @str4 = @str3
                Set @str3 = @str6
        End
        If @tool number = 5
        Begin
                Set @str6 = @str4
                Set @str4 = @str5
                Set @str5 = @str6
        End

        Set @number = 4

End

If CharIndex(@tool_name,@str5) = 1
Begin
        If @tool_number = 1
        Begin
                Set @str6 = @str5
                Set @str5 = @str1
                Set @str1 = @str6
        End
        If @tool_number = 2
        Begin
```

```
                Set @str6 = @str5
                Set @str5 = @str2
                Set @str2 = @str6
        End
        If @tool_number = 3
        Begin
                Set @str6 = @str5
                Set @str5 = @str3
                Set @str3 = @str6
        End
        If @tool_number = 4
        Begin
                Set @str6 = @str5
                Set @str5 = @str4
                Set @str4 = @str6
        End

        Set @number = 5

End

If @number = 0
Begin
        If @tool_number = 1
        Begin
                Set @str5 = @str4
                Set @str4 = @str3
                Set @str3 = @str2
                Set @str2 = @str1
                Set @str1 = NULL
        End

        If @tool_number = 2
        Begin
                Set @str5 = @str4
                Set @str4 = @str3
                Set @str3 = @str2
                Set @str2 = NULL
        End

        If @tool_number = 3
        Begin
                Set @str5 = @str4
                Set @str4 = @str3
                Set @str3 = NULL
        End

        If @tool_number = 4
        Begin
                Set @str5 = @str4
                Set @str4 = NULL
        End

        If @tool_number = 5
```

```
            Begin
                    Set @str5 = NULL
            End

    End

END
GO

SET ANSI_NULLS OFF
GO
SET QUOTED_IDENTIFIER ON
GO

CREATE PROCEDURE [dbo].[report_event]
    @doc ntext
AS

SET NOCOUNT ON

DECLARE @tool_name_1 nvarchar(255)
DECLARE @tool number 1 int

/*
    「Windows セキュリティ正常性検証ツール」のツール名が英語表記の場合、
    または表記が変更となった場合は、以下の定数を変更してください。
*/
Set @tool name 1 = N'Windows セキュリティ正常性検証ツール'
Set @tool_number_1 = 1


DECLARE @idoc int
DECLARE @record_timestamp datetime

DECLARE @str1 nvarchar(max)
DECLARE @str2 nvarchar(max)
DECLARE @str3 nvarchar(max)
DECLARE @str4 nvarchar(max)
DECLARE @str5 nvarchar(max)
DECLARE @tempstr nvarchar(max)

EXEC sp_xml_preparedocument @idoc OUTPUT, @doc

--UTC 時間ではなく、ロケールに合わせた時間を記録します。
--SET @record_timestamp = GETUTCDATE()
SET @record timestamp = GETDATE()

Set @str1 = null
Set @str2 = null
Set @str3 = null
Set @str4 = null
Set @str5 = null

Declare SHR Cursor For
```

```
Select *
From OPENXML(@idoc, '/Event/System-Health-Result')
WITH (
    System_Health_Result1 nvarchar (255) '.'
)

Open SHR
Fetch Next From SHR Into @str1
If @@Fetch_status = 0
    Fetch Next From SHR Into @str2
If @@Fetch_status = 0
    Fetch Next From SHR Into @str3
If @@Fetch_status = 0
    Fetch Next From SHR Into @str4
If @@Fetch_status = 0
    Fetch Next From SHR into @str5
Close SHR
Deallocate SHR

Exec Sort SHR      @tool name 1 , @tool number 1 ,
                         @str1 OUTPUT , @str2 OUTPUT ,
                         @str3 OUTPUT , @str4 OUTPUT ,
                         @str5 OUTPUT
INSERT accounting_data
SELECT
    @record timestamp,
    Computer_Name,
    Event Source,
    MS_MPPE_Encryption_Types,
    MS_Link_Drop_Time_Limit,
    MS Link Utilization Threshold,
    [User_Name],
    NAS_IP_Address,
    NAS Port,
    Service_Type,
    Framed_Protocol,
    Framed IP Address,
    Framed_MTU,
    Class,
    Vendor Specific,
    Called_Station_Id,
    Calling_Station_Id,
    NAS Identifier,
    Acct_Status_Type,
    Acct_Delay_Time,
    Acct Input Octets,
    Acct_Output_Octets,
    Acct_Session_Id,
    Acct Authentic,
    Acct_Session_Time,
    Acct_Input_Packets,
    Acct Output Packets,
    Acct_Terminate_Cause,
    Acct_Multi_Session_Id,
```

```
    Acct_Link_Count,
    Event_Timestamp,
    NAS Port Type,
    Tunnel_Type,
    Tunnel_Medium_Type,
    Tunnel_Client_Endpt,
    Connect_Info,
    Tunnel_Pvt_Group_ID,
    Acct_Interim_Interval,
    NAS_Port_Id,
    Client_IP_Address,
    Client_Vendor,
    MS_CHAP_Domain,
    Authentication Type,
    Client_Friendly_Name,
    SAM_Account_Name,
    Fully Qualifed User Name,
    EAP_Friendly_Name,
    Packet_Type,
    Reason Code,
    MS_RAS_Vendor,
    MS RAS Version,
    NP Policy Name,
    Proxy_Policy_Name,
    Provider Type,
    Provider Name,
    Remote_Server_Address,
    MS RAS Client Name,
    MS_RAS_Client_Version,
    MS_PEAP_Fast_Roamed_Session,
    MS Identity Type,
    MS_Service_Class,
    MS_Quarantine_State,
    @str1,
    @str2,
    @str3,
    @str4,
    @str5,
    Fully_Qualified_Machine_Name,
    MS Network Access Server Type,
    Quarantine_Session_Id,
    Quarantine_Update_Non_Compliant,
    MS Machine Name,
    Machine_Inventory,
    MS_Extended_Quarantine_State,
    @doc ntext
    FROM OPENXML(@idoc, '/Event')
WITH (
    Computer Name nvarchar (255) './Computer-Name',
    Event_Source nvarchar (255) './Event-Source',
    MS_MPPE_Encryption_Types int './MS-MPPE-Encryption-Types',
    MS Link Drop Time Limit int './MS-Link-Drop-Time-Limit',
    MS_Link_Utilization_Threshold int './MS-Link-Utilization-
Threshold',
```

```
    User_Name nvarchar (255) './User-Name',
    NAS_IP_Address nvarchar(15) './NAS-IP-Address',
    NAS Port int './NAS-Port',
    Service_Type int './Service-Type',
    Framed_Protocol int './Framed-Protocol',
    Framed_IP_Address nvarchar(15) './Framed-IP-Address',
    Framed_MTU int './Framed-MTU',
    Class nvarchar (255) './Class',
    Vendor_Specific nvarchar (255) './Vendor-Specific',
    Called_Station_Id nvarchar (255) './Called-Station-Id',
    Calling_Station_Id nvarchar (255) './Calling-Station-Id',
    NAS_Identifier nvarchar (255) './NAS-Identifier',
    Acct_Status_Type int './Acct-Status-Type',
    Acct Delay Time int './Acct-Delay-Time',
    Acct_Input_Octets int './Acct-Input-Octets',
    Acct_Output_Octets int './Acct-Output-Octets',
    Acct Session Id nvarchar (255) './Acct-Session-Id',
    Acct_Authentic int './Acct-Authentic',
    Acct_Session_Time int './Acct-Session-Time',
    Acct Input Packets int './Acct-Input-Packets',
    Acct_Output_Packets int './Acct-Output-Packets',
    Acct Terminate Cause int './Acct-Terminate-Cause',
    Acct Multi Session Id nvarchar (255) './Acct-Multi-Session-Id',
    Acct_Link_Count int './Acct-Link-Count',
    Event Timestamp nvarchar (255) './Event-Timestamp',
    NAS Port Type int './NAS-Port-Type',
    Tunnel_Type int './Tunnel-Type',
    Tunnel Medium Type int './Tunnel-Medium-Type',
    Tunnel_Client_Endpt nvarchar (255) './Tunnel-Client-Endpt',
    Connect_Info nvarchar (255) './Connect-Info',
    Tunnel Pvt Group ID nvarchar (255) './Tunnel-Pvt-Group-ID',
    Acct_Interim_Interval int './Acct-Interim-Interval',
    NAS_Port_Id nvarchar (255) './NAS-Port-Id',
    Client IP Address nvarchar(15) './Client-IP-Address',
    Client_Vendor int './Client-Vendor',
    MS_CHAP_Domain nvarchar (255) './MS-CHAP-Domain',
    Authentication Type int './Authentication-Type',
    Client_Friendly_Name nvarchar (255) './Client-Friendly-Name',
    SAM_Account_Name nvarchar (255) './SAM-Account-Name',
    Fully Qualifed User Name nvarchar (255) './Fully-Qualifed-User-
Name',
    EAP_Friendly_Name nvarchar (255) './EAP-Friendly-Name',
    Packet Type int './Packet-Type',
    Reason_Code int './Reason-Code',
    MS_RAS_Vendor int './MS-RAS-Vendor',
    MS RAS Version nvarchar (255) './MS-RAS-Version',
    NP_Policy_Name nvarchar (255) './NP-Policy-Name',
    Proxy_Policy_Name nvarchar (255) './Proxy-Policy-Name',
    Provider Type int './Provider-Type',
    Provider_Name nvarchar (255) './Provider-Name',
    Remote_Server_Address nvarchar(15) './Remote-Server-Address',
    MS RAS Client Name nvarchar (255) './MS-RAS-Client-Name',
    MS_RAS_Client_Version nvarchar (255) './MS-RAS-Client-Version',
    MS_PEAP_Fast_Roamed_Session int './MS-PEAP-Fast-Roamed-Session',
```

```
    MS_Identity_Type int './MS-Identity-Type',
    MS_Service_Class nvarchar (255) './MS-Service-Class',
    MS Quarantine State int './MS-Quarantine-State',
    Fully_Qualified_Machine_Name nvarchar (255) './Fully-Qualified-
Machine-Name',
    MS_Network_Access_Server_Type int './MS-Network-Access-Server-
Type',
    Quarantine_Session_Id nvarchar (255) './Quarantine-Session-Id',
    Quarantine_Update_Non_Compliant int './Quarantine-Update-Non-
Compliant',
    MS_Machine_Name nvarchar (255) './MS-Machine-Name',
    Machine_Inventory nvarchar (255) './Machine-Inventory',
    MS_Extended_Quarantine_State int './MS-Extended-Quarantine-State'
)

EXEC sp_xml_removedocument @idoc

SET NOCOUNT OFF
GO
```

付録2: ローカル ファイル ログ IAS 形式/SQL Server ログ 出力属性一覧

ローカル ファイル ログ IAS 形式と SQL Server ログに出力される属性とその説明及び各実施ポイントの出力の有無を、要求ログと結果ログ毎に一覧で示します。

ヘッダー情報

各形式で出力されるログのヘッダー情報の一覧は、次の通りです。

ローカル ファイル ログ **IAS** 形式

項目	属性	説明
第 1 項目	NAS-IP-Address	要求を送信している NAS の IP アドレス
第 2 項目	User-Name	アクセスを要求しているユーザーの名前
第 3 項目	Record-Date	ログが書き込まれた日付
第 4 項目	Record-Time	ログが書き込まれた時刻
第 5 項目	Service-Name	RADIUS サーバーで実行されているサービスの名前
第 6 項目	Computer-Name	RADIUS サーバーの名前

SQL Server ログ

項目	属性	説明
第 1 項目	Computer-Name	RADIUS サーバーの名前
第 2 項目	Event-Source	RADIUS サーバーで実行されているサービスの名前

アクセス要求ログ

NPS がクライアントのアクセス要求を受け取った際のログに出力される属性の一覧は、次の通りです。なお、802.1X のログはネットワーク ポリシー サーバーでのみ出力されます。

凡例：N…ネットワーク ポリシー サーバー、実…実施ポイント

■…出力、ー…未出力

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
1	User-Name	ー	ー	ー	ー	■	■	■	■	■	アクセスを要求しているユーザーの名前	IAS 形式では、ヘッダー情報に出力されるのでこの属性は出力されない。 802.1X の場合、クライアントがログオフした状態で接続すると、「host/<コンピュータ名>.<ドメイン名>」の形式でマシン名が出力される。
4	NAS-IP-Address	■	■	■	■	■	■	■	ー	ー	要求元 NAS の IP アドレス	
5	NAS-Port	ー	ー	ー	ー	■	■	■	ー	ー	要求元 NAS の物理ポート番号	
6	Service-Type	■	■	■	■	■	■	■	■	■	ユーザーが要求したサービスの種類	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
7	Framed-Protocol	ー	ー	ー	ー	ー	■	■	ー	ー	使用するプロトコル	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
8	Framed-IP-Address	■	■	ー	ー	ー	ー	ー	ー	ー	要求元 NAS の IP アドレス	
12	Framed-MTU	ー	ー	ー	ー	■	■	■	ー	ー	ユーザー用に構成される転送の最大単位	
25	Class	■	■	■	■	■	■	■	■	■	Access-Accept パケットでクライアントに送信される属性	
30	Called-Station-Id	■	■	ー	ー	■	ー	ー	■	■	アクセス先 ID	

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
31	Calling-Station-Id	■	■	–	–	■	■	■	–	–	アクセス元 ID	
32	NAS-Identifier	■	■	■	■	–	■	■	–	–	要求を送信した NAS を識別する文字列	
44	Acct-Session-Id	■	■	■	■	–	■	■	–	–	サーバー セッションを識別する ID	
61	NAS-Port-Type	■	■	■	■	■	■	■	■	■	要求元 NAS が使用する物理ポートの種類	
64	Tunnel-Type	–	–	–	–	–	■	■	–	–	使用されるトンネリング プロトコル	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
65	Tunnel-Medium-Type	–	–	–	–	–	■	■	–	–	プロトコルのトンネルを作成するときに使うトランスポート メディア	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
66	Tunnel-Client-Endpt	–	–	–	–	–	■	■	–	–	トンネル クライアントの IP アドレス	
77	Connect-Info	–	–	–	–	■	–	–	–	–	確立された接続の種類を指定するために、NAS で使用される情報	
87	NAS-Port-Id	–	–	–	–	■	–	–	–	–	Supplicant を認証する Authenticator のポートを識別する ID	
4108	Client-IP-Address	■	–	■	–	■	■	■	■	–	RADIUS クライアントの IP アドレス	
4116	Client-Vendor	■	–	■	–	■	■	–	■	–	NAS の製造元	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4127	Authentication-Type	■	–	■	–	■	■	–	■	–	ユーザーの検証に使用される認証スキーム	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4128	Client-Friendly-Name	■	–	■	–	■	■	■	■	–	RADIUS クライアントのフレンドリ名	

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
4129	SAM-Account-Name	–	–	–	–	■	■	–	■	–	セキュリティ アカウント マネージャ（SAM） データベースのユーザー アカウント名	
4130	Fully-Qualifed-User-Name	–	–	–	–	■	■	–	■	–	正式な形式のユーザー名	
4132	EAP-Friendly-Name	–	–	–	–	■	■	–	–	–	拡張認証プロトコル（EAP） で使用するフレンドリ名	
4136	Packet-Type	■	■	■	■	■	■	■	■	■	パケットの種類	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4142	Reason-Code	■	■	■	■	■	■	■	■	■	ユーザーを拒否した理由	
4147	MS-RAS-Vendor	–	–	–	–	–	■	■	–	–	RADIUS クライアントマシンのメーカー	
4148	MS-RAS-Version	–	–	–	–	–	■	■	–	–	RADIUS クライアントソフトウェアのバージョン	
4149	NP-Policy-Name	■	–	■	–	■	■	–	■	–	適合したネットワーク ポリシー名	
4154	Proxy-Policy-Name	■	■	■	■	■	■	■	■	■	適合した接続要求ポリシー名	
4155	Provider-Type	■	■	■	■	■	■	■	■	■		値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4156	Provider-Name	–	■	–	■	–	–	■	–	■	接続要求ポリシーで指定した認証プロバイダ名	
4157	Remote-Server-Address	–	■	–	■	–	–	■	–	■	アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス	
4159	MS-RAS-Client-Name	–	–	–	–	–	■	■	–	–	接続を要求したクライアント	

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
4160	MS-RAS-Client-Version	–	–	–	–	–	■	■	–	–	接続を要求したクライアントのバージョン	
8108	MS-Identity-Type	■	■	■	■	–	–	–	–	–	NPS が RADIUS サーバーに対してアクセス要求時に送信する認証	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
8109	MS-Service-Class	■	■	–	–	–	–	–	–	–	IP アドレスを要求する DHCP クライアントを識別する ID	
8111	MS-Quarantine-State	–	–	–	–	■	–	–	–	–	検疫結果	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
8129	Fully-Qualified-Machine-Name	■	–	■	–	■	■	–	■	–	クライアントのフルコンピュータ名	
8132	MS-Network-Access-Server-Type	■	■	■	■	–	■	■	■	■	要求送信元のサーバータイプ	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
8133	Quarantine-Session-Id	■	–	■	–	■	■	–	■	–	クライアントの状態ステートメントを識別する ID	
8138	MS-Machine-Name	■	■	■	■	■	–	–	■	■	クライアントマシン名	
8148	Machine-Inventory	■	–	■	–	■	■	–	■	–	OS のバージョン情報	
8153	MS-Extended-Quarantine-State	–	–	–	–	■	–	–	–	–	NAP の拡張設定により設定した内容	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。

ポリシーチェックの結果ログ

NPS がクライアントのアクセス要求に対してポリシーチェックを行った結果のログに出力される属性の一覧は、次の通りです。なお、802.1X のログはネットワーク ポリシー サーバーでのみ出力されます。

凡例：N…ネットワーク ポリシー サーバー、実…実施ポイント

■…出力、－…未出力

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
6	Service-Type	■	■	■	■	■	■	■	■	■	ユーザーが要求したサービスの種類	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
7	Framed-Protocol	■	■	■	■	■	■	■	■	■	使用するプロトコル	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
25	Class	■	■	■	■	■	■	■	■	■	Access-Accept パケットでクライアントに送信される属性	
26	Vendor-Specific	－	－	－	－	－	－	－	■	■	独自の NAS 機能のサポートに使用される属性	
44	Acct-Session-Id	■	■	■	■	－	■	■	－	－	サーバー セッションを識別する ID	
64	Tunnel-Type	－	－	－	－	■	－	－	－	－	使用されるトンネリング プロトコル	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
65	Tunnel-Medium-Type	－	－	－	－	■	－	－	－	－	プロトコルのトンネルを作成するときに使うトランスポート メディア	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
81	Tunnel-Pvt-Group-ID	－	－	－	－	■	－	－	－	－	VLAN を識別する文字列	
85	Acct-Interim-Interval	－	－	－	－	■	－	－	－	－	Interim パケット送信間隔	
4108	Client-IP-Address	■	－	■	－	■	■	－	■	－	RADIUS クライアントの IP アドレス	

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
4116	Client-Vendor	■	–	■	–	■	■	–	■	–	NAS の製造元	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4120	MS-CHAP-Domain	–	–	–	–	–	■	■	–	–	認証に使用されたドメイン名	16 進 Ascii で、「（start of heading）<ドメイン名>」を表す。
4127	Authentication-Type	■	–	■	–	■	■	–	■	–	ユーザーの検証に使用される認証スキーム	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4128	Client-Friendly-Name	■	–	■	–	■	■	–	■	–	RADIUS クライアントのフレンドリ名	
4129	SAM-Account-Name	–	–	–	–	■	■	–	■	–	セキュリティ アカウント マネージャ（SAM） データベースのユーザー アカウント名	
4130	Fully-Qualifed-User-Name	–	–	–	–	■	■	–	■	–	正式な形式のユーザー名	
4132	EAP-Friendly-Name	–	–	–	–	■	■	–	–	–	拡張認証プロトコル（EAP） で使用するフレンドリ名	
4136	Packet-Type	■	■	■	■	■	■	■	■	■	パケットの種類	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
4142	Reason-Code	■	■	■	■	■	■	■	■	■	ユーザーを拒否した理由	
4149	NP-Policy-Name	■	–	■	–	■	■	–	■	–	適合したネットワーク ポリシー名	
4154	Proxy-Policy-Name	■	■	■	■	■	■	■	■	■	適合した接続要求ポリシー名	
4155	Provider-Type	■	■	■	■	■	■	■	■	■		値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。

属性 ID	属性	DHCP		正常性登録機関（IPSec）		802.1X	VPN		TS ゲートウェイ		説明	備考
		N	実	N	実	N	N	実	N	実		
4156	Provider-Name	–	■	–	■	–	–	■	–	■	接続要求ポリシーで指定した認証プロバイダ名	
4157	Remote-Server-Address	–	■	–	■	–	–	■	–	■	アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス	
8100	MS-PEAP-Fast-Roamed-Session	–	–	–	–	■	■	–	–	–	無線のアクセスポイントを使用時など、Full 認証ではなく、前回分の認証情報を用いて認証を行う事を示す ID	
8111	MS-Quarantine-State	■	■	■	■	■	■	■	■	■	検疫結果	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
8124	System-Health-Result	■	–	■	–	■	■	–	■	–	クライアントから送信された、クライアントの状態と準拠状態	
8129	Fully-Qualified-Machine-Name	■	–	■	–	■	■	–	■	–	クライアントのフルコンピュータ名	
8133	Quarantine-Session-Id	■	–	■	–	■	■	–	■	–	クライアントの状態ステートメントを識別する ID	
8136	Quarantine-Update-Non-Compliant	■	–	■	–	■	■	–	■	–	自動修復の ON、OFF を表す ID	
8138	MS-Machine-Name	–	–	–	–	■	■	■	–	–	クライアントマシン名	
8148	Machine-Inventory	■	–	■	–	■	■	–	■	–	OS のバージョン情報	
8153	MS-Extended-Quarantine-State	■	■	■	■	■	■	■	■	■	NAP の拡張設定により設定した内容	値は属性値 ID で出力される。詳細については P.61「付録 3:属性と属性値一覧表」を参照。
-87	MS-Link-Drop-Time-Limit	–	–	–	–	■	■	■	–	–	活用されていないリンクを破棄するまでの時間	
-86	MS-Link-Utilization-Threshold	–	–	–	–	■	■	■	–	–	利用可能な帯域幅の割合	

付録3: 属性と属性値一覧表

属性によっては値が属性値で出力されるものと属性値 ID で出力されるものがあります。NAP の検疫操作で出力される属性の説明および属性 ID と属性値 ID の対応表を、ローカル ファイル ログ データベース互換形式で出力される順に、下記に示します。なお、すべての属性の定義については、「C:\Windows\System32\ias」にある属性定義ファイル「dnary.xml」で確認することができます。

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
ヘッダー情報	1	ComputerName	RADIUS サーバーの名前	
ヘッダー情報	2	ServiceName	RADIUS サーバーで実行されているサービスの名前	
ヘッダー情報	3	Record-Date	ログが書き込まれた日付	
ヘッダー情報	4	Record-Time	ログが書き込まれた時刻	
4136	5	Packet-Type	パケットの種類	· 1 = Access-Request · 2 = Access-Accept · 3 = Access-Reject · 4 = Accounting-Request · 5 = Accounting-Response · 11 = Access-Challenge · 12 = Status-Server （experimental） · 13 = Status-Client （experimental） · 255 = Reserved
1	6	User-Name	アクセスを要求しているユーザーの名前	
4130	7	Fully-Qualified-User-Name	正式な形式のユーザー名	
30	8	Called-Station-ID	アクセス元 ID	
31	9	Calling-Station-ID	アクセス先 ID	
19	10	Callback-Number	コールバック電話番号	

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
8	11	Framed-IP-Address	要求元 NAS の IP アドレス	
32	12	NAS-Identifier	要求を送信した NAS を識別する文字列	
4	13	NAS-IP-Address	要求元 NAS の IP アドレス	
5	14	NAS-Port	要求元 NAS の物理ポート番号	
4116	15	Client-Vendor	NAS の製造元	· 0 = RADIUS Standard · 1 = Proteon · 5 = ACC · 9 = Cisco · 14 = BBN · 15 = Xylogics, Inc. · 43 = 3Com · 52 = Cabletron Systems · 64 = Gandalf · 117 = Telebit · 166 = Shiva Corporation · 181 = ADC Kentrox · 244 = Lantronix · 272 = BinTec Communications GmbH · 307 = Livingston Enterprises, Inc. · 311 = Microsoft · 332 = Digi International · 343 = Intel Corporation · 429 = U.S. Robotics, Inc. · 434 = EICON · 529 = Ascend Communications Inc. · 562 = Nortel Networks
4108	16	Client-IP-Address	RADIUS クライアントの IP アドレス	
4128	17	Client-Friendly-Name	RADIUS クライアントのフレンドリ名	
55	18	Event-Timestamp	このイベントが NAS で発生した日付と時刻	
62	19	Port-Limit	NAS がユーザーに提供する最大ポート数	
61	20	NAS-Port-Type	要求元 NAS が使用する物理ポート	· 0 = 非同期 （モデム）

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
			の種類	· 1 = 同期 （T1 回線） · 2 = ISDN 同期 · 3 = ISDN 非同期 V.120 · 4 = ISDN 非同期 V.110 · 5 = 仮想 （VPN） · 6 = PIAFS · 7 = HDLC クリア チャネル · 8 = X.25 · 9 = X.75 · 10 = G.3 Fax · 11 = SDSL - 対称型 DSL · 12 = ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation · 13 = ADSL-DMT - Asymmetric DSL Discrete Multi-Tone · 14 = IDSL - ISDN デジタル加入者回線 · 15 = イーサネット · 16 = DSL - 不明な種類のデジタル加入者回線 · 17 = ケーブル · 18 = ワイヤレス - その他 · 19 = ワイヤレス - IEEE 802.11 · 20 = トークン リング · 21 = FDDI
77	21	Connect-Info	確立された接続の種類を指定するために、NAS で使用される情報	
7	22	Framed-Protocol	使用するプロトコル	· 1 = PPP · 2 = SLIP · 3 = AppleTalk Remote Access Protocol （ARAP） · 4 = Gandalf Proprietary SingleLink/MultiLink protocol · 5 = Xylogics proprietary IPX/SLIP · 6 = X.75 Synchronous · 256 = MPP · 257 = EURAW · 258 = EUUI · 259 = X25 · 260 = COMB · 261 = FR
6	23	Service-Type	ユーザーが要求したサービスの種類	· 1 = Login · 2 = Framed

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
				· 3 = Callback Login · 4 = Callback Framed · 5 = Outbound · 6 = Administrative · 7 = NAS Prompt · 8 = Authenticate Only · 9 = Callback Nas Prompt · 10 = Call Check · 11 = Callback Administrative · 12 = Authorize only
4127	24	Authentication-Type	ユーザーの検証に使用される認証スキーム	· 1 = PAP · 2 = CHAP · 3 = MS-CHAP v1 · 4 = MS-CHAP v2 · 5 = EAP · 7 = 非認証 · 8 = 拡張子 · 9 = MS-CHAP v1 CPW · 10 = MS-CHAP v2 CPW · 11 = ー
4149	25	NP-Policy-Name	適合したネットワークポリシー名	
4142	26	Reason Code	ユーザーを拒否した理由	· 00 = 成功 · 01 = 内部エラー · 02 = アクセス拒否 · 03 = 誤った形式の要求 · 04 = グローバル カタログは利用不可 · 05 = ドメインは利用不可 · 06 = サーバーは利用不可 · 07 = そのようなドメインはありません · 08 = そのようなユーザーは存在しません · 16 = 認証エラー · 17 = パスワードの変更エラー · 18 = サポートされていない認証の種類 · 19 = ユーザー アカウントに対して可逆暗号化パスワードは保存されていません · 32 = ローカル ユーザーのみ · 33 = パスワードを変更する必要があります · 34 = アカウントは無効

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
				· 35 = アカウントの期限切れ · 36 = アカウントのロックアウト · 37 = 無効なログオン時間 · 38 = アカウントの制限 · 48 = リモート アクセス ポリシーに一致しません · 49 = 接続要求ポリシーに一致しません · 64 = ダイヤルインのロックアウト · 65 = ダイヤルインは無効 · 66 = 無効な認証の種類 · 67 = 無効な呼び出し元 · 68 = 無効なダイヤルイン時間 · 69 = 無効な呼び出し先 · 70 = 無効なポートの種類 · 71 = 無効な制限 · 80 = レコードがありません · 96 = セッションのタイムアウト · 97 = 予期しない要求
25	27	Class	Access-Accept パケットでクライアントに送信される属性	
27	28	Session-Timeout	セッション終了までの時間の長さ（秒単位）	
28	29	Idle-Timeout	セッション終了までのアイドル時間の長さ（秒単位）	
29	30	Termination-Action	サービス完了時に NAS が行う動作	· 0 = Default · 1 = RADIUS-Request
4132	31	EAP-Friendly-Name	拡張認証プロトコル（EAP）で使用するフレンドリ名	
40	32	Acct-Status-Type	アカウンティング パケットがブリッジ接続、ルーティング、またはターミナル サーバー セッションを起動するか、停止するかを指定する番号	· 1 = Start · 2 = Stop · 3 = Interim Update · 7 = Accounting-On · 8 = Accounting-Off · 9 = Tunnel-Start · 10 = Tunnel-Stop · 11 = Tunnel-Reject · 12 = Tunnel-Link-Start · 13 = Tunnel-Link-Stop

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
				· 14 = Tunnel-Link-Reject · 15 = Failed
41	33	Acct-Delay-Time	NAS が同じアカウンティング パケットを送信していた時間の長さ（秒単位）	
42	34	Acct-Input-Octets	セッション中に受信したオクテット数	
43	35	Acct-Output-Octets	セッション中に送信したオクテット数	
44	36	Acct-Session-ID	サーバー セッションを識別する ID	
45	37	Acct-Authentic	着信呼び出しを認証したサーバーを指定する番号	· 0 = None · 1 = RADIUS · 2 = Local · 3 = Remote
46	38	Acct-Session-Time	セッションがアクティブであった時間の長さ（秒単位）	
47	39	Acct-Input-Packets	セッション中に受信したパケット数	
48	40	Acct-Output-Packets	セッション中に送信したパケット数	
49	41	Acct-Terminate-Cause	接続が終了した理由	· 1 = User-Request · 2 = Lost-Carrier · 3 = Lost-Service · 4 = Idle-Timeout · 5 = Session-Timeout · 6 = Admin-Reset · 7 = Admin-Reboot · 8 = Port-Error · 9 = NAS-Error · 10 = NAS-Request · 11 = NAS-Reboot · 12 = Port-Unneeded · 13 = Port-Preempted · 14 = Port-Suspended · 15 = Service-Unavailable · 16 = Callback · 17 = User-Error

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
				· 18 = Host-Request · 19 = Supplicant-Restart · 20 = Reauthentication-Failure · 21 = Port-Reinit · 22 = Port-Disabled
50	42	Acct-Multi-SSN-ID	マルチリンク セッションを識別する ID	
51	43	Acct-Link-Count	マルチリンク セッションでのリンクの数	
85	44	Acct-Interim-Interval	NAS が送信する各中間更新間隔の長さ（秒単位）	
64	45	Tunnel-Type	使用されるトンネリング プロトコル	· 1 = Point-to-Point Tunneling Protocol （PPTP） · 2 = Layer Two Forwarding （L2F） · 3 = Layer Two Tunneling Protocol （L2TP） · 4 = Ascend Tunnel Management Protocol （ATMP） · 5 = Virtual Tunneling Protocol （VTP） · 6 = IP Authentication Header in the Tunnel-mode （AH） · 7 = IP-in-IP Encapsulation （IP-IP） · 8 = Minimal IP-in-IP Encapsulation （MIN-IP-IP） · 9 = IP Encapsulating Security Payload in the Tunnel-mode （ESP） · 10 = Generic Route Encapsulation （GRE） · 11 = Bay Dial Virtual Services （DVS） · 12 = IP-in-IP Tunneling · 13=Virtual LANs （VLAN）
65	46	Tunnel-Medium-Type	プロトコルのトンネルを作成するときに使うトランスポート メディア	· 1 = IP （IP version 4） · 2 = IP6 （IP version 6） · 3 = NSAP · 4 = HDLC （8-bit multidrop） · 5 = BBN 1822 · 6 = 802 （includes all 802 media plus Ethernet canonical format） · 7 = E.163 （POTS） · 8 = E.164 （SMDS Frame Relay ATM） · 9 = F.69 （Telex） · 10 = X.121 （X.25 Frame Relay） · 11 = IPX · 12 = Appletalk

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
				· 13 = Decnet IV · 14 = Banyan Vines · 15 = E.164 with NSAP format subaddress
66	47	Tunnel-Client-Endpt	トンネル クライアントの IP アドレス	
67	48	Tunnel-server-Endpt	トンネル サーバーの IP アドレス	
68	49	Acct-Tunnel-Connection	トンネルに割り当てられた識別子	
81	50	Tunnel-Pvt-Group-ID	特定のトンネリング セッションのグループ ID	
82	51	Tunnel-Assignment-ID	セッションを割り当てるトンネル	
83	52	Tunnel-Preference	アクセス サーバーで複数のトンネルの種類がサポートされている場合に、Tunnel-Type 属性で示されるトンネルの種類の優先順位を示す数値	
4134	53	MS-Acct-Auth-Type	ダイヤルアップユーザーの認証方法	
4135	54	MS-Acct-EAP-Type	ダイヤルアップユーザーの認証に使用した拡張認証プロトコル（EAP）	
4148	55	MS-RAS-Version	RADIUS クライアントソフトウェアのバージョン	
4147	56	MS-RAS-Vendor	RADIUS クライアントマシンのメーカー	
4121	57	MS-CHAP-Error	MS-CHAP トランザクションを説明するエラー データ	
4120	58	MS-CHAP-Domain	認証に使用されたドメイン名	
-90	59	MS-MPPE-Encryption-Types	MPPE と使用可能な暗号化のタイプ	
-89	60	MS-MPPE-Encryption-Policy	暗号化の使用が許可されているのか、または必須として要求されているのかを示す ID	· 1 = Encryption-Allowed · 2 = Encryption-Required
4154	61	Proxy-Policy-Name	適合した接続要求ポリシー名	

属性 ID	データベース互換形式出力順	属性	説明	記録される属性値の意味
4155	62	Provider-Type	認証の種類	· 0 = None · 1 = Windows · 2 = RADIUS Proxy
4156	63	Provider-Name	接続要求ポリシーで指定した認証プロバイダ名	
4157	64	Remote-Server-Address	アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス	
4159	65	MS-RAS-Client-Name	接続を要求したクライアント	
4160	66	MS-RAS-Client-Version	接続を要求したクライアントのバージョン	
8108	データベース互換形式での出力なし	MS-Identity-Type	検疫の種類	1 = Machine health check
8111	データベース互換形式での出力なし	MS-Quarantine-State	検疫結果	0 = Full Access 1 = Quarantine 2 = Probation
8132	データベース互換形式での出力なし	MS-Network-Access-Server-Type	実施ポイントの種類	0 = 指定なし 1 = ターミナル サーバー ゲートウェイ 2 = リモート アクセス サーバー (VPN - ダイヤルアップ) 3 = DHCP サーバー 5 = 正常性登録機関
8153		MS-Extended-Quarantine-State	HCAP(Host Credential Authorization Protocol) で利用される検疫結果	0 = No Data 1 = Transition 2 = Infected 3 = Unknown

付録4: イベント ログ（セキュリティ）一覧

検疫操作で出力されたイベント ログの詳細について、次に示します。

[ID 6272] イベント ログ

イベント要素		説明
キーワード	成功の監査	
タスクのカテゴリ	ネットワークポリシーサーバー	
説明	ネットワーク ポリシー サーバーがユーザーにアクセスを許可しました。	
ユーザー:	セキュリティ ID:	ユーザー名、またはユーザーSID
	アカウント名:	アクセスを要求しているユーザーの名前
	アカウント ドメイン:	ドメイン名
	完全修飾アカウント名:	正式な形式のユーザー名
クライアント コンピュータ:	セキュリティ ID:	クライアントマシンのフルコンピュータ名
	アカウント名:	クライアントマシンのコンピュータ名 出力形式：<コンピュータ名>.<ドメイン名>
	完全修飾アカウント名:	クライアントマシンのフルコンピュータ名
	OS バージョン:	OS のバージョン情報
	被呼端末 ID:	アクセス先 ID
	起呼端末 ID:	アクセス元 ID
NAS:	NAS IPv4 アドレス:	要求元 NAS の IPv4 アドレス
	NAS IPv6 アドレス:	要求元 NAS の IPv6 アドレス
	NAS ID:	要求を送信した NAS を識別する文字列
	NAS ポートの種類:	要求元 NAS が使用する物理ポートの種類
	NAS ポート:	要求元 NAS の物理ポート番号
RADIUS クライアント:	クライアントのフレンドリ名:	RADIUS クライアントのフレンドリ名

イベント要素		説明
	クライアント IP アドレス:	RADIUS クライアントの IP アドレス
認証の詳細:	プロキシ ポリシー名:	適合した接続要求ポリシー名
	ネットワーク ポリシー名:	適合したネットワークポリシー名
	認証プロバイダ:	
	認証サーバー:	アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス
	認証の種類:	ユーザーの検証に使用される認証スキーム
	EAP の種類:	拡張認証プロトコル （EAP） で使用するフレンドリ名
	アカウントのセッション ID:	サーバー セッションを識別する ID
検疫情報:	結果:	検疫結果
	セッション ID:	クライアントの状態ステートメントを識別する ID

[ID 6273] イベント ログ

イベント要素		説明
キーワード	失敗の監査	
タスクのカテゴリ	ネットワークポリシーサーバー	
説明	ネットワーク ポリシー サーバーがユーザーのアクセスを拒否しました。	
ユーザー:	セキュリティ ID:	ユーザー名、またはユーザーSID
	アカウント名:	アクセスを要求しているユーザーの名前
	アカウント ドメイン:	ドメイン名
	完全修飾アカウント名:	正式な形式のユーザー名
クライアント コンピュータ:	セキュリティ ID:	クライアントマシンのフルコンピュータ名
	アカウント名:	クライアントマシンのコンピュータ名 出力形式：<コンピュータ名>.<ドメイン名>
	完全修飾アカウント名:	クライアントマシンのフルコンピュータ名
	OS バージョン:	OS のバージョン情報
	被呼端末 ID:	アクセス先 ID

イベント要素		説明
	起呼端末 ID:	アクセス元 ID
NAS:	NAS IPv4 アドレス:	要求元 NAS の IPv4 アドレス
	NAS IPv6 アドレス:	要求元 NAS の IPv6 アドレス
	NAS ID:	要求を送信した NAS を識別する文字列
	NAS ポートの種類:	要求元 NAS が使用する物理ポートの種類
	NAS ポート:	要求元 NAS の物理ポート番号
RADIUS クライアント:	クライアントのフレンドリ名:	RADIUS クライアントのフレンドリ名
	クライアント IP アドレス:	RADIUS クライアントの IP アドレス
認証の詳細:	プロキシ ポリシー名:	適合した接続要求ポリシー名
	ネットワーク ポリシー名:	適合したネットワークポリシー名
	認証プロバイダ:	
	認証サーバー:	アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス
	認証の種類:	ユーザーの検証に使用される認証スキーム
	EAP の種類:	拡張認証プロトコル （EAP） で使用するフレンドリ名
	アカウントのセッション ID:	サーバー セッションを識別する ID
	理由コード:	ユーザーを拒否した理由を示す ID
	理由:	ユーザーを拒否した理由の詳細

[ID 6274] イベント ログ

イベント要素		説明
キーワード	失敗の監査	
タスクのカテゴリ	ネットワークポリシーサーバー	
説明	ネットワーク ポリシー サーバーがユーザーの要求を破棄しました。	
ユーザー:	セキュリティ ID:	ユーザー名、またはユーザーSID
	アカウント名:	アクセスを要求しているユーザーの名前
	アカウント ドメイン:	ドメイン名
	完全修飾アカウント名:	正式な形式のユーザー名

イベント要素		説明
クライアント コンピュータ:	セキュリティ ID:	クライアントマシンのフルコンピュータ名
	アカウント名:	クライアントマシンのコンピュータ名 出力形式：<コンピュータ名>.<ドメイン名>
	完全修飾アカウント名:	クライアントマシンのフルコンピュータ名
	OS バージョン:	OS のバージョン情報
	被呼端末 ID:	アクセス先 ID
	起呼端末 ID:	アクセス元 ID
NAS:	NAS IPv4 アドレス:	要求元 NAS の IPv4 アドレス
	NAS IPv6 アドレス:	要求元 NAS の IPv6 アドレス
	NAS ID:	要求を送信した NAS を識別する文字列
	NAS ポートの種類:	要求元 NAS が使用する物理ポートの種類
	NAS ポート:	要求元 NAS の物理ポート番号
RADIUS クライアント:	クライアントのフレンドリ名:	RADIUS クライアントのフレンドリ名
	クライアント IP アドレス:	RADIUS クライアントの IP アドレス
認証の詳細:	プロキシ ポリシー名:	適合した接続要求ポリシー名
	ネットワーク ポリシー名:	適合したネットワークポリシー名
	認証プロバイダ:	
	認証サーバー:	アクセス要求を転送したネットワークポリシー サーバーの IP アドレス
	認証の種類:	ユーザーの検証に使用される認証スキーム
	EAP の種類:	拡張認証プロトコル （EAP） で使用するフレンドリ名
	アカウントのセッション ID:	サーバー セッションを識別する ID
	理由コード:	ユーザーを拒否した理由を示す ID
	理由:	ユーザーを拒否した理由の詳細

[ID 6276] /[ID 6278]イベント ログ

イベント要素		説明
キーワード	成功の監査	
タスクのカテゴリ	ネットワークポリシーサーバー	

イベント要素			説明
説明	[ID 6276]	ネットワーク ポリシー サーバーがユーザーを検疫しました。	
	[ID 6278]	ホストが定義済みの正常性ポリシーを満たしていたため、ネットワーク ポリシー サーバーはユーザーにフル アクセスを許可しました。	
ユーザー:	セキュリティ ID:		ユーザー名、またはユーザーSID
	アカウント名:		アクセスを要求しているユーザーの名前
	アカウント ドメイン:		ドメイン名
	完全修飾アカウント名:		正式な形式のユーザー名
クライアント コンピュータ:	セキュリティ ID:		クライアントマシンのフルコンピュータ名
	アカウント名:		クライアントマシンのコンピュータ名 出力形式：<コンピュータ名>.<ドメイン名>
	完全修飾アカウント名:		クライアントマシンのフルコンピュータ名
	OS バージョン:		OS のバージョン情報
	被呼端末 ID:		アクセス先 ID
	起呼端末 ID:		アクセス元 ID
NAS:	NAS IPv4 アドレス:		要求元 NAS の IPv4 アドレス
	NAS IPv6 アドレス:		要求元 NAS の IPv6 アドレス
	NAS ID:		要求を送信した NAS を識別する文字列
	NAS ポートの種類:		要求元 NAS が使用する物理ポートの種類
	NAS ポート:		要求元 NAS の物理ポート番号
RADIUS クライアント:	クライアントのフレンドリ名:		RADIUS クライアントのフレンドリ名
	クライアント IP アドレス:		RADIUS クライアントの IP アドレス
認証の詳細:	プロキシ ポリシー名:		適合した接続要求ポリシー名
	ネットワーク ポリシー名:		適合したネットワークポリシー名
	認証プロバイダ:		
	認証サーバー:		アクセス要求を転送したネットワーク ポリシー サーバーの IP アドレス

イベント要素		説明
	認証の種類:	ユーザーの検証に使用される認証スキーム
	EAP の種類:	拡張認証プロトコル （**EAP**） で使用するフレンドリ名
	アカウントのセッション **ID**:	サーバー セッションを識別する **ID**
検疫情報:	結果:	検疫結果
	拡張結果:	**NAP** の拡張設定により設定した内容
	セッション **ID**:	クライアントの状態ステートメントを識別する **ID**
	ヘルプ **URL**:	
	システム正常性検証ツールの結果:	クライアントから送信された、クライアントの状態と準拠状態

付録5: 参考情報

本書を参照するにあたっては、併せて次のドキュメントもご参照下さい。

No.	Source	URL
1.	Step-by-Step Guide: Demonstrate NAP DHCP Enforcement in a Test Lab	http://www.microsoft.com/downloads/details.aspx?FamilyID=ac38e5bb-18ce-40cb-8e59-188f7a198897&displaylang=en
2.	Step-by-Step Guide: Demonstrate NAP IPSec Enforcement in a Test Lab	http://www.microsoft.com/downloads/details.aspx?FamilyID=298ff956-1e6c-4d97-a3ed-7e7ffc4bed32&displaylang=en
3.	Step-by-Step Guide: Demonstrate NAP 802.1X Enforcement in a Test Lab	http://www.microsoft.com/downloads/details.aspx?familyid=8A0925EE-EE06-4DFB-BBA2-07605EFF0608&displaylang=en
4.	Step-by-Step Guide: Demonstrate NAP VPN Enforcement in a Test Lab	http://www.microsoft.com/downloads/details.aspx?familyid=729BBA00-55AD-4199-B441-378CC3D900A7&displaylang=en
5.	Windows Server 2008 TS Gateway Server Step-By-Step Setup Guide	http://www.microsoft.com/downloads/details.aspx?FamilyID=518d870c-fa3e-4f6a-97f5-acaf31de6dce&DisplayLang=en
6.	Windows Server 2008 Technical Library > Troubleshooting > Events and Errors > NAP Infrastructure	http://technet2.microsoft.com/windowsserver2008/en/library/b502f974-d99a-43d3-8e37-a631bf2f66321033.mspx
7.	Interpret Windows System Health Validator Entries in Log Files	http://technet2.microsoft.com/windowsserver2008/en/library/8da6b148-e912-4013-8fd5-d738eea8e5ed1033.mspx
8.	Interpret NPS Database Format Log Files	http://technet2.microsoft.com/windowsserver2008/en/library/75872f64-d4ca-494d-a9cf-4ba053331ca01033.mspx