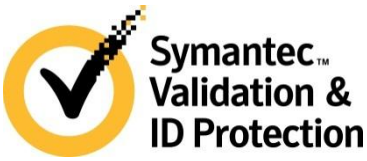
# Symantec Validation and ID Protection （VIP）
# ネットワークポリシー
Version: 2.1
発効日: 2011 年 9 月 7 日



【注意】
本書は、シマンテックが https://www.verisign.com/repository/VIP/VIP_Policy_2.1.pdf で公開しているネットワークポリシーを参考のために翻訳したものです。お客様を何ら拘束するものではございません。また、シマンテックは本書をもって、お客様に対し、何らの表明・保証をおこなうものではございません。実際にお客様に適用されるネットワークポリシーは、上記ホームページで公開している情報となりますので、予めご承知おきください。

# 1 はじめに

Symantec Validation and ID Protection ネットワーク（VIP ネットワーク）は、アプリケーションのセキュリティ強化、ならびに利用者の個人情報保護の強化のため、より強固な認証の普及に積極的に取り組むオンラインサービスプロバイダと企業のネットワークである。Symantec が運営する VIP ネットワークでは、参加企業は二要素認証クレデンシャルを共有できる。つまり、利用者は、参加 企業が運営する VIP 対応のウェブサイトであれば、どのウェブサイトにおいても、1 個の二要素認証クレデンシャルを共有できることとする。

二要素認証の利用により、VIP ネットワークでは金融資産情報、秘密情報、個人を特定できる情報のセキュリティの向上が可能である。VIP ネットワークは、VIP ネットワークに参加するウェブサイトにとっては、 盗まれた情報が悪用されてユーザのオンラインアカウントに不正にログインされる危険性を大幅に低減 するという利点がある。また、利用者にとっては、犯罪者が推測および盗んだユーザ名やパスワードを 使用してサービスにログインすることができないという安心感を与える。

VIP ネットワークでは Symantec が運営する共有検証インフラストラクチャを使用するため、参加企業は自 前の認証インフラストラクチャをすべて管理・運営するような負担を負わずとも、二要素認証クレデンシャルの配布や運用が可能となる。VIP ネットワークでは、デバイス 1 個で複数のウェブサイトでの取引を保 護できるため、利用者は日常的に強固な認証を簡単に利用できる。

本文書、『Symantec Validation and ID Protection（VIP）ネットワークポリシー （「ポリシー」）』は、VIP ネットワークに適用される主要ポリシーをまとめたものである。本ポリシーは、VIP ネットワーク内で二要素認証クレデンシャルを発行、使用、管理するための業務要件、法的要件、技術的要件を規定する。本ポリシー内で使用する用語は、特段の規定がある場合、または文脈により他の意 味であることが明白な場合を除き、本ポリシー末尾の用語集で規定する意味を有するものとする。

# 2 VIP ネットワーク参加者と相関関係

## 2.1 VIP ネットワーク参加者

本項では、VIP ネットワークにおける様々な参加者（以降、「VIP 参加者」）の定義と、VIP ネットワークにおける各 VIP 参加者の役割について説明する。各 VIP 参加者の義務詳細については後述する。

### 2.1.1 ネットワークオペレータ

ネットワークオペレータは、VIP ネットワークでの VIP クレデンシャルの使用をサポートするセキュアなインフラストラクチャを提供、管理する。VIP ネットワークおよび本ポリシーにおいては、Symantec がネットワークオペレータの役割を担う。

### 2.1.2 依拠当事者

依拠当事者とは、二要素認証としての VIP クレデンシャルを受入れる個人または組織である。任意の VIP クレデンシャルを受入れるためには、依拠当事者は、利用者からの要求があり次第、ネットワークオ ペレータと調整して、その VIP クレデンシャルをアクティベーションし、依拠当時者のローカルディレクトリもしくは保有する利用者情報内にある当該利用者のユーザ ID にバインドする。VIP ネットワークで共有さ れるのは第 2 認証要素のみなので、依拠当事者は利用者に対して、依拠当事者固有のユーザ ID もしく は第 1 認証要素も提供しなければならない。通常、ユーザ ID は、依拠当事者のウェブサイトに登録され ている、利用者に関連付けられたユーザ名やパスワードである。

依拠当事者は、自ウェブサイトで使用できるように（ネットワークオペレータと調整して）アクティベーションしローカルディレクトリにバインドした VIP クレデンシャルについて、ライフサイクル管理を行うものとする。

依拠当事者は、（自らがアクティベーションした VIP クレデンシャルに関して）自ウェブサイトで使用される VIP クレデンシャルに関連のあるクレデンシャルライフサイクル管理全般の責任を負うものとする。依拠 当事者は、自ウェブサイトでの利用者の行為に関して、管理する権限を有するとともに責任を負うものとする。

### 2.1.3 クレデンシャル発行者

クレデンシャル発行者は、VIP ネットワークで VIP クレデンシャルを発行する権限を持つ個人または組織 である。

VIP ネットワークでは、クレデンシャル発行者は依拠当事者を兼ね、さらに他の VIP 参加者が発行した VIP クレデンシャルを受入れる必要がある。ただし、かかる VIP 参加者が VIP クレデンシャルをアクティ ベーションおよびバインドするサイトを持たないと判定された場合はこの要件を除外する。本条件におい ては、VIP 参加者は依拠当事者の役割から除外される。ただし、かかる VIP 参加者がクレデンシャル発 行者となった後、VIP クレデンシャルのアクティベーションおよびバインドの能力を有した場合、かかる VIP 参加者は依拠当事者の役割を担うことを要求される。

VIP ネットワークにおいて、Symantec が発行する VIP クレデンシャルに関しては、Symantec はクレデン シャル発行者としての役割を担い、本ポリシーに規定されたクレデンシャル発行者の義務を負うものとする。

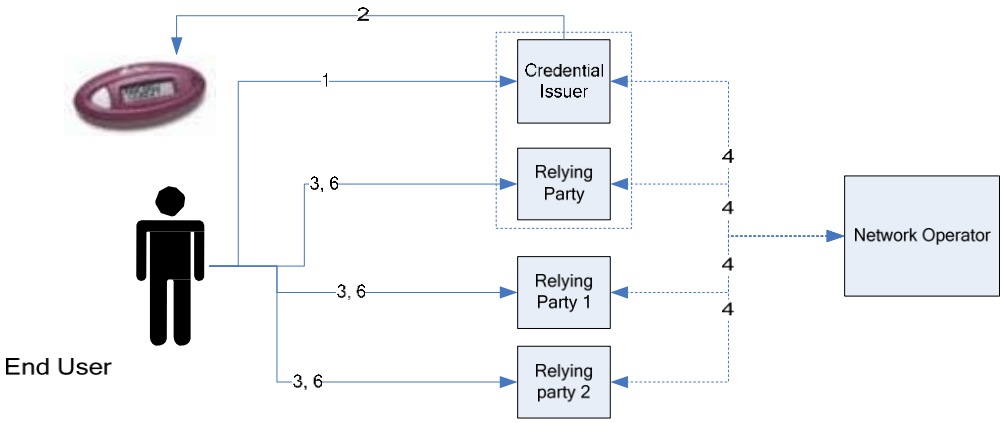
### 2.1.4 利用者

利用者とは、VIP クレデンシャルを正当に所有する個人である。各利用者は、VIP クレデンシャルの使用を予定しているウェブサイトの依拠当事者とともに、VIP クレデンシャルのアクティベーションとバインドを 調整する必要がある。

## 2.2 VIP 参加者の相関関係

依拠当事者は、VIP ネットワークに参加した後、VIP クレデンシャルを受入れ可能となるように一部またはすべてのインターネットアプリケーションを構成し、オンライン取引のセキュリティを向上させるために 一部またはすべての利用者に VIP クレデンシャルの取得を推奨する。VIP クレデンシャルはクレデンシャル発行者から取得する。利用者が取得した VIP クレデンシャルは、依拠当事者によるアクティベーションおよびバインドの完了を以って、VIP ネットワーク上のすべての依拠当事者に受け入れられるものとする。

下図に VIP ネットワーク上の様々な VIP 参加者の相関関係を示す。




End user: 利用者
Credential Issuer: クレデンシャル発行者
Relying Party: 依拠当事者
Network Operator: ネットワークオペレータ
図 1: Symantec VIP ネットワークの運用

Symantec VIP ネットワークのワークフロー

ステップ 1: 利用者は、クレデンシャル発行者に VIP クレデンシャルの利用申請を行う。

ステップ 2: クレデンシャル発行者は、利用者に VIP クレデンシャルを配布する。

ステップ 3: 利用者は、依拠当事者のサイトにおいて、VIP クレデンシャルのアクティベーションおよび自らのユーザ ID とのバインドをオンラインで要求する。

ステップ 4: 依拠当事者は、自ウェブサイトでの利用を可能にするために、VIP クレデンシャルのアクティベーションをネットワークオペレータに要求する。

ステップ 5: 依拠当事者は、自ウェブサイトにおいて、VIP クレデンシャルを利用者のユーザ ID にバインドする。

ステップ 6: 利用者は、この依拠当事者のウェブサイトにおいて、VIP クレデンシャルの使用が可能となる。

利用者と依拠当事者の間で VIP クレデンシャルのアクティベーションとバインドを行う際、利用者は、固有の VIP クレデンシャル ID およびワンタイムパスワードの値（入力は 1 度か 2 度）だけでなく、第 1 認証要素情報を提示する。利用者は VIP クレデンシャルの使用を希望するサイト毎に、アクティベーションとバインドのプロセスを繰り返し行う。VIP クレデンシャルのアクティベーションと、依拠当事者側でのローカルユーザ ID へのバインドが完了すると、利用者は、より強固な認証のために、第 1 要素 ID とともに第 2 要素のワンタイムパスワードの値を依拠当事者に提示する。依拠当事者は、検証のために、利用者が提示した VIP クレデンシャル ID とワンタイムパスワードの値をネットワークオペレータに提示する。

# 3 VIP クレデンシャル

## 3.1 VIP クレデンシャル

VIP クレデンシャルは、共有鍵と固有の VIP クレデンシャル ID から構成される。共有鍵は、利用者が物理的に所有するデバイス内に保護された状態で格納される。VIP クレデンシャル ID は、VIP

クレデンシャル製造業者と VIP クレデンシャル自体を識別する、12～16 文字の英数字からなる文字列で構成される。VIP クレデンシャル ID は、クレデンシャルとネットワークオペレータの両方で共有される。デバイスは、既 知のアルゴリズムと VIP クレデンシャルを使用してワンタイムパスワードの値を生成する。デバイスが生 成したワンタイムパスワードとネットワークオペレータがそのクレデンシャル ID について生成したワンタイムパスワードの値を比較し、これらの値が同一であればその VIP クレデンシャルは有効と判定される。VIP クレデンシャルは匿名であり、アクティベートする依拠当事者のウェブサイトのローカルユーザ ID に バインドされた際に第 2 認証要素となる。

VIP ネットワークは、他の二要素認証クレデンシャル同様に OATH（Initiative for Open Authentication）をサポートする。VIP ネットワークで特定のデバイスをサポートするには、Symantec がそのデバイスを正式に認定することが必要となる。VIP ネットワークは、VIP クレデンシャルをはじめとする様々な種類のデバイスをサポートするように設計されている。VIP クレデンシャルは、専用セキュリティハードウェアデバイスなどに格納することも可能であり、携帯電話、フラッシュストレージデバイス、クレジットカードなどの 利用者向けのデバイスに格納することも可能である。

## 3.2 VIP クレデンシャルの所持証明

各 VIP クレデンシャルは、固有の識別子である VIP クレデンシャル ID と、VIP クレデンシャル所持の証 明に使用できる認証機能（ワンタイムパスワードなど）を有する。

## 3.3 VIP クレデンシャルのプロビジョニングおよび保護

### 3.3.1 VIP クレデンシャルのプロビジョニング

デバイスには、製造中または製造後のダイナミックプロビジョニングによって用意された VIP クレデンシャルが格納される。尚、デバイス外から VIP クレデンシャルにはアクセスできない様に考慮されている必要がある。製造中のデバイスに VIP クレデンシャルを用意する場合、製造業者は以下の 2 つのプロセスの いずれかを使用する。

1. デバイス製造業社は、Symantec に VIP クレデンシャルをセキュアに要求する。ネットワークオペ レータである Symantec は、各デバイス向けに暗号化した形態の VIP クレデンシャルを返し、暗号化した形態の VIP クレデンシャルのコピーを保管する。

2. デバイス製造業社は、VIP クレデンシャルを生成し、暗号化し、セキュアに Symantec に送信する。ネットワークオペレータである Symantec は、暗号化された形態の VIP クレデンシャルのコピーを保管する。

これらの VIP クレデンシャルは、利用者を認証するためのワンタイムパスワードの値を生成する際に製造後のダイナミックプロビジョニングプロセスを使用してデバイスのプロビジョニングを行う場合、利用者は最初にクレデンシャル発行者からプロビジョニングコードを取得する必要がある。利用者は、デバイスのワンタイムパスワードアプリケーションにプロビジョニングコードを入力します。プロビジョニング要求がネットワークオペレータのダイナミックプロビジョニングサービスにセキュアに送信され、それから VIP クレデンシャルがデバイスにセキュアに送信される。

### 3.3.2 VIP クレデンシャルの保護

ネットワークオペレータは、上記の VIP クレデンシャルのプロビジョニングプロセスの一環として、暗号化された形態の VIP クレデンシャルのコピーを、ネットワークオペレータのデータセンターにセキュアに保管する。VIP クレデンシャルはトリプル DES 暗号化アルゴリズムを使用して暗号化される。

## 3.4 クレデンシャルのステータス

VIP クレデンシャルは、ローカルステータスとグローバルステータスを所有する。下表にて、依拠当事者によって VIP ネットワーク上で VIP クレデンシャルに関連付けられる様々なローカルステータスと、個々のステータスが VIP クレデンシャルの利用にどのように影響を及ぼすかを示す。

| ステータス | 説明 |
|---|---|
| *New* | VIP クレデンシャルは発行されているが、アクティベーションやバインドは完了していない状態。 |
| *Enabled （Active）* | 依拠当事者が利用者の要求に応じて VIP クレデンシャルのアクティベーションとバインドを完了している状態。VIP クレデンシャルはその依拠当事者により利用可能な状態である。 |
| *Inactive* | VIP クレデンシャルは依拠当事者によって利用を停止されている状態。その依拠当事者が将来この VIP クレデンシャルを利用可能とするためには、本ポリシーに従って VIP クレデンシャルを再度アクティベート、バインドする必要がある。 |
| *Locked* | VIP クレデンシャルは、特定の依拠当事者による認証が連続して何度も失敗した後ロックされており、その依拠当事者による利用ができない状態。その依拠当事者が将来この VIP クレデンシャルを利用可能とするためには、本ポリシーに従って VIP クレデンシャルのロックを解除する必要がある。 |
| *Disabled* | VIP クレデンシャルは、依拠当事者によって一時的に無効化されており、その依拠当事者による利用ができない状態。その依拠当事者が将来この VIP クレデンシャルを使用可能とするためには、本ポリシーに従って VIP クレデンシャルを再度有効にする必要がある。VIP クレデンシャルが無効化されている間は、その依拠当事者は認証に使用する一時的なパスワードを設定可能である。 |

表 1:クレデンシャルローカルステータスの説明

下図にて、クレデンシャルのローカルステータスとその遷移を図示する。

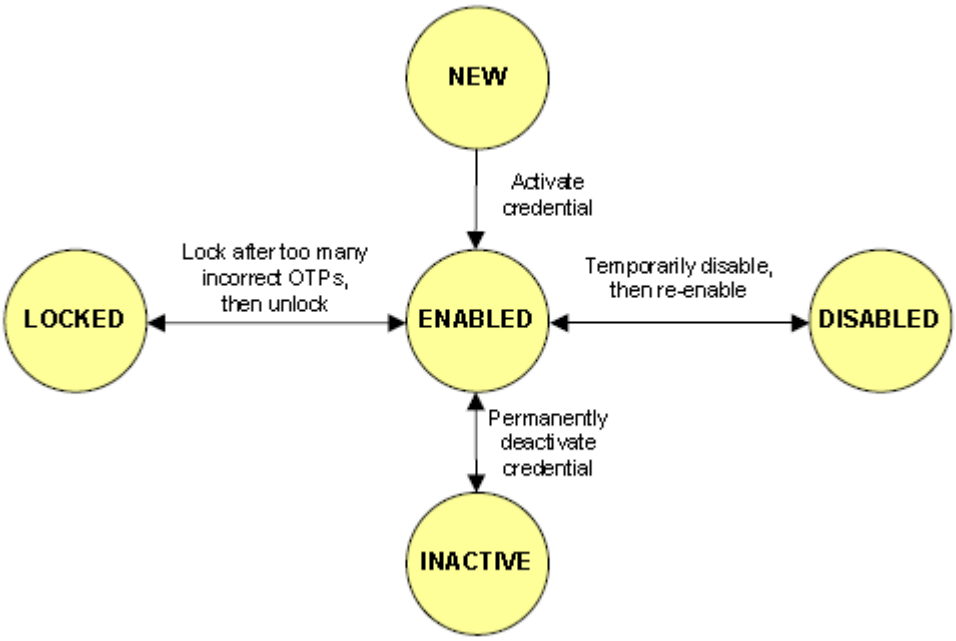



図 2 クレデンシャルのローカルステータスの遷移

下表にて、VIP ネットワークにおいて VIP クレデンシャルに関連付けられるグローバルステータスと、個々のステータスが VIP ネットワーク上での全 VIP 参加者の VIP クレデンシャルの利用にどのように影響を及ぼすかを示す。

| ステータス | 説明 |
|---|---|
| *Valid* | VIP クレデンシャルは、任意の VIP 参加者によって利用可能な状態。VIP 参加者がどのようにこのクレデンシャルを使用できるかは、前述のローカルステータスに応じて異なる。 |
| *Revoked* | VIP クレデンシャルは、ネットワークオペレータによって失効されており、VIP ネットワークの全 VIP 参加者によって利用不可能な状態。 |

表 2: クレデンシャルのグローバルステータスの説明

## 3.5 クレデンシャルの検証プロセス

VIP クレデンシャルを使用するために、利用者が、VIP クレデンシャルのアクティベーションプロセスを完了し、依拠当事者のウェブサイトにバインドすると、その依拠当事者のウェブサイトは、二要素認証のために、利用者に対して VIP クレデンシャルのワンタイムパスワードの値を提示するように指示する。利用者がワンタイムパスワードの値を提示すると、依拠当事者はその利用者に関連付けられた VIP クレデンシャル ID をローカルディレクトリで検索し、認証のためにネットワークオペレータに VIP クレデンシャル ID とワンタイムパスワードを転送する。ネットワークオペレータは、依拠当事者のウェブサイトに有効または無効のメッセージを返す。

## 3.6 クレデンシャルのライフサイクル管理

VIP クレデンシャルのプロビジョニングが完了して利用者に発行されると、かかる依拠当事者はその VIP クレデンシャルをアクティベート、バインドすることが可能となる。各依拠当事者は、自

らがアクティベーションおよびバインドの調整を行う全ての VIP クレデンシャルのライフサイクルを管理する責任を負う。

次項では、全ての VIP クレデンシャルに関連する主な「クレデンシャルライフサイクル管理」について説明する。VIP ネットワークにおいて、依拠当事者は VIP ネットワークにおける VIP クレデンシャルに関する正し いステータスが常時反映を保証する責任を負うものする。ただし、依拠当事者は、他の依拠当事者のウェブサイトで使用される VIP クレデンシャルについては、ライフサイクル管理の責任を負わないものとする。ネットワークオペレータは、VIP ネットワーク上のあらゆる VIP クレデンシャルの全クレデンシャルライフサイクル管理を行う権利を有するものとする。

クレデンシャルのライフサイクル管理に関して下記に記述する。

### 3.6.1 アクティベーション

アクティベーションは、特定の依拠当事者が VIP ネットワーク上で VIP クレデンシャルを有効化するプロセスである。アクティベーション行為自体では利用者のユーザ ID と VIP クレデンシャルをリンクしない。依拠当事者が VIP クレデンシャルをアクティベートすると、その依拠当事者はその後そのクレデンシャル のバインドが可能となる。

#### 3.6.1.1 アクティベーション要求者

各依拠当事者が、VIP クレデンシャルを認証、アクティベートするためには、ネットワークオペレータにアクティベーション要求を送信する必要がある。依拠当事者でもあるクレデンシャル発行者は、自らが発行する VIP クレデンシャルを事前にアクティベートすることができ、自ウェブサイトにある利用者のユーザ ID と VIP クレデンシャルを事前にバインドすることが可能である。

#### 3.6.1.2 VIP クレデンシャルのアクティベーションの責任者

ネットワークオペレータが、VIP ネットワークで VIP クレデンシャルをアクティベートできる唯一の VIP 参加者となる。

#### 3.6.1.3 アクティベーションの要件

VIP ネットワークで VIP クレデンシャルをアクティベートさせるためには、利用者が VIP クレデンシャルを所有していることを依拠当事者に対して証明する必要がある。クレデンシャル発行者が事前にアクティベートした VIP クレデンシャルの場合は、この要件は適用されない。

### 3.6.2 ロック/ロック解除

VIP クレデンシャルのロックは、特定の依拠当事者に関して VIP クレデンシャルのステータスを [Enabled] から[Locked]に変更するプロセスである。依拠当事者は、ロックされた VIP クレデンシャルのロックが解 除されるまでそのクレデンシャルを利用不可とする。特定の依拠当事者に関して VIP クレデンシャルがロックされた場合、その他の依拠当事者のウェブサイトにおいては、その VIP クレデンシャルは利用可能で ある。

#### 3.6.2.1 VIP クレデンシャルのロックが必要な状況

依拠当事者が VIP クレデンシャルの検証に連続して失敗すると、その依拠当事者に関して VIP クレデンシャルがロックされる。

たとえば、ワンタイムパスワードトークンタイプの VIP クレデンシャルの場合、特定の依拠当事者が VIP クレデンシャルで連続して誤ったワンタイムパスワードを入力すると、その依拠当事者の VIP クレデンシ ャルがロックされる。ワンタイムパスワードの値を受信する依拠当事者はワンタイムパスワードの認証失敗回数のしきい値を設定できるが、VIP クレデンシャルのロックに遷移させる認証失敗回数は 10 回を超過しないことが推奨される。

#### 3.6.2.2 VIP クレデンシャルのロック責任者

ネットワークオペレータのみが、特定の依拠当事者がＶＩＰ クレデンシャルの認証に連続して失敗した後、 かかる依拠当事者に関して当該ＶＩＰ クレデンシャルをロック可能である。

#### 3.6.2.3 VIP クレデンシャルのロック解除要求者

当該 VIP クレデンシャルにバインドされたアカウントを所有する利用者のみが、ロックされた VIP クレデンシャルのロック解除要求をネットワークオペレータに送信するように依拠当事者に要求可能である。

#### 3.6.2.4 VIP クレデンシャルのロック解除責任者

ネットワークオペレータのみが、VIP クレデンシャルに関する依拠当事者の要求を受信して、かかる VIP クレデンシャルのロックを解除可能である。

#### 3.6.2.5 VIP クレデンシャルのロック解除要件

ネットワークオペレータのみが、依拠当事者からロック解除要求を受信後、その依拠当事者に関して VIP クレデンシャルのロックを解除可能である。依拠当事者は、利用者のユーザ ID を十分確認したうえ、上 記第 3.2 項に従ってその利用者がかかるＶＩＰ クレデンシャルを所有していることを確認した後、ロック解 除要求を送信するものとする。

### 3.6.3 無効化/有効化

VIP クレデンシャルの無効化は、特定の依拠当事者に関して、VIP クレデンシャルのステータスを一時的に[Enabled]から[Disabled]に変更するプロセスである。その依拠当事者は、無効化された VIP クレデン シャルが再度有効化されるまで、そのクレデンシャルを使用不可とする。依拠当事者は、無効化された VIP クレデンシャルの代わりに、かかるＶＩＰ クレデンシャルが無効化されている間ワンタイムパスワード の代わりに使用できる一時的なパスワードを設定する事が可能である。

#### 3.6.3.1 VIP クレデンシャルの無効化が必要な状況

特定の依拠当事者に関して、VIP クレデンシャルの無効化が必要な状況には、以下のようなものがある。

- o 一時的に、利用者が VIP クレデンシャルを所持しない状態で依拠当事者のウェブサイトにアク セスする必要があるとき。
- o VIP クレデンシャルが動作せず、VIP クレデンシャルの交換を待つ間に利用者が依拠当事者の ウェブサイトにアクセスする必要があるとき。
- o 利用者がＶＩＰ クレデンシャルの危殆の懸念を報告し、VIP クレデンシャルの交換を待つ間に依 拠当事者のウェブサイトにアクセスする必要があるとき。

#### 3.6.3.2 クレデンシャルの無効化要求者

VIP クレデンシャルの利用者は、依拠当事者に関するＶＩＰ クレデンシャルの無効化要求をネットワーク オペレータに送信するようにその依拠当事者に要求可能である。

依拠当事者は、無効化要求が本ポリシーの条項で保証されていると自己の裁量によって判断できる場 合、その依拠当事者に関して VIP クレデンシャルを無効化するように直接ネットワークオペレータに要求 可能である。

ネットワークオペレータは、無効化が本ポリシーの条項で保証されていると自己の裁量によって

判断でき る場合、特定の依拠当事者に関して VIP クレデンシャルを無効化可能である。

#### 3.6.3.3 VIP クレデンシャルの無効化

責任者 ネットワークオペレータのみが、特定の依拠当事者に関して VIP クレデンシャルを無効化可能である。各依拠当事者は、本ポリシー第 4.2.2.5 項に従って、VIP クレデンシャルの誤用があった場合、これを報告 する義務を負う。

#### 3.6.3.4 クレデンシャルの再有効化責任者

VIP クレデンシャルの利用者のみが、無効化された VIP クレデンシャルの再有効化要求をネットワークオ ペレータに送信するように依拠当事者に要求可能である。ネットワークオペレータは、依拠当事者から VIP クレデンシャルの再有効化要求を受信した場合のみ、その依拠当事者に関して VIP クレデンシャル の再有効化が可能である。依拠当事者は、（i）利用者のユーザ ID を二要素認証で十分確認し、（ii）上記 第 3.2 項に従って、利用者が VIP クレデンシャルを所有していることを確認し、（iii）VIP クレデンシャルが 無効化された理由が VIP ネットワークに危険を及ぼす可能性ではないことを確認した後にのみ、再有効 化要求を送信するものとする。

### 3.6.4 ワンタイムパスワードのみの VIP クレデンシャルの同期化

同期化を利用することで、ワンタイムパスワードのみの VIP クレデンシャルの VIP ネットワーク上の同期 化や再同期化が可能である。

#### 3.6.4.1 同期が必要な状況

ワンタイムパスワードが VIP ネットワーク上で検証されることなくイベントベースの VIP クレデンシャルで生成される場合や、タイムベースの VIP クレデンシャルが長期間 VIP ネットワーク上で検証されない場合、VIP クレデンシャルとネットワークオペレータが同期しなくなることがある。

#### 3.6.4.2 VIP クレデンシャルの同期化

責任者 利用者から再同期化要求を受信した際、該当する依拠当事者はかかる利用者の VIP クレデンシャルの再同期化をネットワークオペレータに要求する。依拠当事者が、 （i）利用者のユーザ ID を二要素認証で 十分確認し、（ii）上記第 3.2 項に従って、利用者が VIP クレデンシャルを所有していることを確認した後にのみネットワークオペレータによる VIP クレデンシャルの再同期化を要求可能である。

### 3.6.5 VIP クレデンシャルの停止

VIP クレデンシャルの停止は、特定の依拠当事者に関して、VIP クレデンシャルのステータスを [Enabled]、[Locked]、[Disabled]から[Inactive]に変更するプロセスである。その依拠当事者は再度アクティベートされるまで、その VIP クレデンシャルを利用不可とする。

#### 3.6.5.1 停止が必要な状況

特定の依拠当事者に関して、VIP クレデンシャルの停止が必要な状況には、以下のようなものがある。

- VIP クレデンシャルの使用方法が本ポリシーに反するとき。
- 利用者が VIP クレデンシャルの紛失、盗難、破損を報告したとき。
- 利用者が依拠当事者との関係を終了したとき。
- 利用者が依拠当事者に関して VIP クレデンシャルを使用することを希望しなくなったとき。

- VIP クレデンシャルが作動しなくなったとき。
- 利用者が VIP クレデンシャルの危殆の懸念を報告したとき。
- VIP ネットワークでその VIP クレデンシャルを引き続き使用することが VIP ネットワークに危険を 及ぼす可能性があると判断されたとき。

#### 3.6.5.2 VIP クレデンシャルの停止要求者

VIP クレデンシャルの利用者は、VIP ネットワーク上での依拠当事者に関する VIP クレデンシャルの停止 要求をネットワークオペレータに送信するように、その依拠当事者に要求可能である。

依拠当事者は、停止要求が本ポリシーの条項で保証されていると自己の裁量で判断できる場合、VIP ネットワーク上でその依拠当事者に関して VIP クレデンシャルを停止するように直接ネットワークオペレータに要求可能である。

ネットワークオペレータは、停止が本ポリシーの条項で保証されていると自己の裁量で判断できる場合、VIP ネットワーク上で VIP クレデンシャルを停止可能である。

#### 3.6.5.3 VIP クレデンシャルの停止責任者

特定の VIP クレデンシャルのアクティベーションを担当した依拠当事者は、VIP ネットワーク上でのその 依拠当事者の使用に関してかかる VIP クレデンシャルの停止をネットワークオペレータに要求可能である。ネットワークオペレータは任意の VIP ネットワーク参加者の任意の VIP クレデンシャルを停止可能で ある。各依拠当事者は、本ポリシー第 4.2.2.5 項に従って、任意の VIP クレデンシャルの誤用がある場合、 これを報告する義務を負う。

### 3.6.6 VIP クレデンシャルの失効

VIP クレデンシャルの失効は、VIP ネットワーク上で VIP クレデンシャルのグローバルステータスを[Valid] から[Revoked]に変更するプロセスである。いかなる依拠当事者も、失効された VIP クレデンシャルを VIP ネットワーク上で使用することはできない。

#### 3.6.6.1 失効が必要な状況

VIP クレデンシャルの失効が必要な状況には、以下のようなものがある。

- VIP クレデンシャルの使用方法が本ポリシーに反するとき。
- 利用者が VIP クレデンシャルの紛失、盗難、破損を報告し、ネットワークオペレータが合理的に これを確認できたとき。
- クレデンシャル発行者が VIP クレデンシャルの紛失、盗難、破損を報告し、ネットワークオペレー タが合理的にこれを確認できたとき。
- VIP クレデンシャルが作動しなくなったとき。
- VIP クレデンシャルに危殆が発生したとき。
- VIP ネットワークでその VIP クレデンシャルを引き続き使用することが VIP ネットワークに危険を 及ぼす可能性があると、ネットワークオペレータの裁量で判断されたとき。

#### 3.6.6.2 失効要求者

VIP クレデンシャルの利用者は、VIP ネットワーク上の VIP クレデンシャル失効要求をネットワーク

オペレ ータに送信するように、VIP クレデンシャルを発行したクレデンシャル発行者または VIP クレデンシャルと 利用者のユーザ ID をバインドした依拠当事者に要求可能である。

VIP クレデンシャルを発行したクレデンシャル発行者または VIP クレデンシャルと利用者のユーザ ID を バインドした依拠当事者は、取消要求が本ポリシーの条項で保証されていると自己の裁量で判断できる 場合、VIP ネットワーク上の VIP クレデンシャルの失効を直接ネットワークオペレータに要求可能である。

ネットワークオペレータは、本ポリシーの条項で失効が保証されていると自己の裁量で判断した場合、VIP ネットワーク上の VIP クレデンシャルを失効可能である。

#### 3.6.6.3 VIP クレデンシャルの失効責任者

ネットワークオペレータのみが、VIP ネットワークで VIP クレデンシャルを失効可能である。 各依拠当事者は、本ポリシー第 4.2.2.5 項に従って、VIP クレデンシャルの誤用があった場合、これを報告する義務を負う。

# 4 役割と責任

## 4.1 ネットワークオペレータ

ネットワークオペレータは、VIP ネットワークにおける VIP クレデンシャルの使用を支援するセキュアなインフラストラクチャを運営し、本項記載の要件を遵守するものとする。VIP ネットワークおよび本ポリシー においては、Symantec がネットワークオペレータである。

### 4.1.1 セキュリティ要件

ネットワークオペレータは、VIP ネットワークをセキュアに運営するためのポリシーおよび手続を確定する 責任を負い、VIP ネットワークの完全性を保護するために必要であると自己の裁量で判断した場合、任 意の処置を講じることが可能である。本要件には、VIP 参加者による VIP ネットワークの誤用や VIP クレ デンシャルの不正使用の検出、被疑が生じた場合に、VIP 参加者のシャットダウンあるいは VIP クレデン シャルを失効する権利も含まれる。

ネットワークオペレータは、システムのセキュリティを確保して VIP ネットワークソフトウェアおよびデータ ファイルを不正なアクセスから保護するために、商業的に合理的と考えられる方策を講じるものする。ベ リサインは毎年、データセンターについて SAS 70 Type II（監査基準書第 70 号）の監査を行っている。 最新の SAS 70 Type II 監査報告書は、任意のクレデンシャル発行者または依拠当事者の要求に応じて 提供される。

### 4.1.2 運用要件

#### 4.1.2.1 VIP 参加者およびデバイスの認定

ネットワークオペレータは以下の責任を負う。

- VIP ネットワークで VIP クレデンシャルとともに使用する各種デバイスの認定
- VIP ネットワークにおけるクレデンシャル発行者および依拠当事者の認定

#### 4.1.2.2 ネットワークの運営

ネットワークオペレータは、以下を行うものとする。

- VIP ネットワークにおいて VIP クレデンシャルをアクティベートするものとする。

- 現在の VIP クレデンシャルのステータス（[enabled]、[disabled]、[locked]など）に関する（利用者 以外の）VIP 参加者のあらゆる要求に応じるものとする。

- VIP ネットワーク上の VIP クレデンシャルの最新のステータスを維持、伝達するものとする。

- ワンタイムパスワードの値を検証するものとする。

- 依拠当事者の代理として、クレデンシャルの全ライフサイクル管理を実行するものとする。

### 4.1.3 プライバシー要件

#### 4.1.3.1 プライバシーポリシー

ネットワークオペレータは、プライバシーに関する適用法規に準拠するプライバシーポリシーを維持するものとする。

Symantec は、Symantec アイデンティティプロテクションセンターを通じて、クレデンシャル発行者であると同時にネットワークオペレータとしても VIP ネットワークに参加する。Symantec は、クレデンシャル発行 者として、利用者の個人情報を入手する。Symantec がクレデンシャル発行者として入手した利用者の個人情報は、Symantec のプライバシーポリシーおよびプライバシーに関する適用法規の支配を受けるも のとする。

#### 4.1.3.2 個人情報として取り扱われる情報

ネットワークオペレータは VIP クレデンシャルに関連付けられたいかなる利用者の個人情報も入手しないものとする。ネットワークオペレータが各 VIP クレデンシャルについて保持するのは、匿名で、いかなる 利用者の個人情報を含まない共有鍵と VIP クレデンシャル ID に限られる。ただし、ネットワークオペレータは、VIP クレデンシャルを検証するために VIP ネットワーク上で使用する VIP クレデンシャル識別情報を、個人情報として取扱い、これらの情報はネットワークオペレータのプライバシーポリシーの支配を受 けるものとする。

尚、VIP クレデンシャルステータス情報（[enabled]、[inactive]等）は個人情報とはみなさないものとする。

### 4.1.4 責任

ネットワークオペレータは、VIP クレデンシャルを VIP ネットワークで検証する際、VIP クレデンシャルが VIP ネットワークで有効であること、要求している依拠当事者に関して有効化されていること、VIP クレデンシャルが生成したワンタイムパスワードの値が VIP クレデンシャル ID に関連付けられていることを判 定する。Symantec は、VIP クレデンシャルに関していかなる陳述も行わず、Symantec の管理の範囲外 での VIP クレデンシャルの使用に関連する損害に対して責任を負わないものとする。

## 4.2 依拠当事者

依拠当事者とは、本ポリシーの条項に準ずる VIP クレデンシャルを受入れる任意の個人または組織である。依拠当事者は、本項記載の要件を遵守するものとする。

### 4.2.1 セキュリティ要件

依拠当事者は、秘密の質問/回答やアウトオブバンドの認証をはじめとする適切な認証手段により、ユー ザを正しく識別することが可能である。

依拠当事者は、以下の手段により利用者の情報を保護するものとする。

- SSL （Secure Socket Layer）技術をはじめとするセキュアなチャネルを使用して、すべてのログ イン情報を保護すること。

- VIP クレデンシャルと利用者のユーザ ID のバインド情報が格納された自己のネットワークのセキュリティを保護すること。依拠当事者は、最低限ファイアウォールを使用して自己のネットワークを内外からの侵入から保護し、システムにアクセスするネットワーク活動の特性および送信元 を制御するものとする。

### 4.2.2 運用要件

#### 4.2.2.1 ネットワーク参加要件

依拠当事者は、利用者が VIP クレデンシャルを要求するあらゆる場所に VIP ロゴを明確に表示することによって、VIP ネットワークで認定された依拠当事者であることを表明する責任を負う。さらに、依拠当事者は、ネットワークオペレータが保持、公表する任意の認定 VIP 参加者リストに掲載されることに同意する。

#### 4.2.2.2 クレデンシャルのアクティベーション

依拠当事者は、VIP クレデンシャルを VIP ネットワークで使用するためにアクティベートする際、以下を行うものとする。

- 必要な利用者識別情報をすべて入手する。

- 必要な VIP クレデンシャル識別情報をすべて入手する。

- ネットワークオペレータが提示する形態と実質的に同様の形態で VIP クレデンシャル使用条件 に合意するように利用者に要求する。

- VIP クレデンシャル識別情報の検証要求を Symantec にセキュアに送信し、VIP ネットワークで のその依拠当事者に関する VIP クレデンシャルのアクティベーションを要求する。

#### 4.2.2.3 クレデンシャルの管理

依拠当事者は、VIP ネットワークで使用するために（ネットワークオペレータと調整して）自らがアクティベートしてバインドした VIP クレデンシャルを厳密に管理する責任を負う。これらの責任には、以下のもの がある。

- VIP クレデンシャルが不正利用された場合、または不正利用の疑いがある場合、VIP クレデンシャルの紛失や盗難の報告があった場合、利用者からの要求があった場合に、速やかに VIP クレデンシャルを無効化または停止する。

- 自らがアクティベーションを要求してバインドした VIP クレデンシャルの利用者に対して、第一次 サポートを提供する。

- 利用者が自分の VIP クレデンシャルを管理する手段を提供する。

- 第 3.6 項に記載の、クレデンシャルの全ライフサイクル管理機能を提供する。

#### 4.2.2.4 クレデンシャルの依拠

依拠当事者はすべての有効な VIP クレデンシャルを受入れるものとする。依拠当事者は、VIP クレデン シャルに依拠する前に、まず VIP ネットワークで使用できるようネットワークオペレータとともに VIP クレデンシャルのアクティベーションを調整するものとする。次に、依拠当事者は、VIP クレデンシャルと自己のシステム内の利用者のユーザ ID をバインドする。

依拠当事者は、VIP クレデンシャルに依拠する際、VIP クレデンシャルとは別の第 1 認証手段を使用す るものとする。

#### 4.2.2.5 誤用の報告

依拠当事者は、VIP クレデンシャルの不正利用された場合または不正利用の疑いがある場合、VIP クレデンシャルの紛失や盗難の通知があった場合に、ネットワークオペレータに報告するものとする。

#### 4.2.2.6 代替認証手段

紛失、破損、その他の理由で利用者が VIP クレデンシャルを使用できない場合、依拠当事者はその利用者を認証する代替手段を提供する必要がある。依拠当事者は、その利用者に関して新たな VIP クレデンシャルのアクティベーションが完了するか、もとの VIP クレデンシャルが再度使用可能になるまで、その利用者のユーザ ID を検証して自ウェブサイトへのアクセスを許可するためのセキュアな機能を提供するものとする。

利用者のユーザ ID は、当該組織のセキュリティポリシーに応じて、以下の例をはじめとする様々な方法 で検証可能である。

- 事前定義の秘密の質問に対する回答
- 利用者のアウトオブバンド認証
- 対面確認（銀行の支店等）

これらの方法で発行した一時的なパスワードは 7 日を超えて有効としないものとする。7 日経過後は新し いー時的なパスワードを発行する必要がある。

### 4.2.3 プライバシー

#### 4.2.3.1 プライバシーポリシー

依拠当事者は、プライバシーに関する適用法規に準拠するプライバシーポリシーを維持するものとする。

#### 4.2.3.2 個人情報として取扱われる情報

VIP クレデンシャルのアクティベーションや利用者情報とのバインドの過程で、利用者が依拠当事者に提 示する全ての情報は、個人情報として取り扱われ、依拠当事者のプライバシーポリシーの支配を受ける ものとする。

尚、VIP クレデンシャルのステータス情報は個人情報とは見なさないものとする。

### 4.2.4 責任

依拠当事者は、自らがアクティベートして利用者のユーザ ID とバインドさせた有効な VIP クレデンシャルに依拠する責任を負うものとする。

## 4.3 クレデンシャル発行者

クレデンシャル発行者は、VIP ネットワークで使用する VIP クレデンシャルを発行する個人または組織である。クレデンシャル発行者は本項記載の要件を遵守するものとする。

### 4.3.1 セキュリティ要件

クレデンシャル発行者は、以下の手段により利用者情報のセキュリティを保証するものとする。

- SSL （Secure Socket Layer）技術をはじめとするセキュアなチャネルを使用して、クレデンシャル発行の目的で利用者が提示したすべてのデータを保護すること。

- 自己のネットワークのセキュリティを保護すること。クレデンシャル発行者は、最低限ファイアウォールを使用して自己のネットワークを内外からの侵入から保護し、システムにアクセスするネットワーク活動の特性および送信元を制御するものとする。

### 4.3.2 運用要件

#### 4.3.2.1 ネットワーク参加要件

クレデンシャル発行者は、VIP ロゴを以下のように明確に表示することによって、VIP ネットワークで認定 されたクレデンシャル発行者であることを表明する責任を負う。

- 利用者に VIP サービスを提供するあらゆる場所に VIP ロゴを表示する。

- クレデンシャル発行者が発行した VIP クレデンシャルを搭載したデバイスに VIP ロゴを表示する。

さらに、クレデンシャル発行者は、ネットワークオペレータが保持、公表する認定 VIP 参加者リストに掲載 されることに同意する。

#### 4.3.2.2 クレデンシャルの発行

クレデンシャル発行者は、利用者に VIP クレデンシャルを発行する際、以下を行うものとする。

- 必要な利用者識別情報をすべて入手する。

- 必要な VIP クレデンシャル識別情報をすべて入手する。

- ネットワークオペレータが提示する形態と実質的に同様の形態で VIP クレデンシャル使用条件 に合意するように利用者に要求する。

### 4.3.3 プライバシー要件

#### 4.3.3.1 プライバシーポリシー

クレデンシャル発行者は、プライバシーに関する適用法規に準拠するプライバシーポリシーを維持するものとする。

#### 4.3.3.2 個人情報として取り扱われる情報

VIP クレデンシャル入手過程で、利用者がクレデンシャル発行者に提示する全ての情報は、個人情報と して取り扱われ、クレデンシャル発行者のプライバシーポリシーの支配を受けるものとする。

### 4.3.4 責任

クレデンシャル発行者は、利用者に有効な VIP クレデンシャルを提供する責任を負うものとする。クレデンシャル発行者は、VIP クレデンシャルに関していかなる陳述も行わず、発行サービス提供時に本ポリシーに従って作業する限り、有効な VIP クレデンシャルの使用に関連する損害に対して責任を負わないも のとする。

### 4.4 利用者

VIP クレデンシャルの利用者は、有効な VIP クレデンシャルの発行先である。

#### 4.4.1 セキュリティ要件

利用者は自己の VIP クレデンシャルのセキュリティの責任を負うものとする。利用者は最低限、以下を行うものとする。

- 必ず、第 1 認証データとは別に VIP クレデンシャルを保管する。
- VIP クレデンシャルの紛失、盗難、その他の危殆が発生した場合、クレデンシャル発行者または依拠当事者に通知する。

#### 4.4.2 利用者の義務

利用者は最低限、以下を行うものとする。

- VIP クレデンシャル入手時に、クレデンシャル発行者に正確な情報を提供する。
- VIP クレデンシャルのアクティベーション時に、依拠当事者に正確な情報を提供する。
- 合法的な目的のみに VIP クレデンシャルを使用する。
- VIP で認定された依拠当事者のウェブサイトでのみ VIP クレデンシャルを使用する。

#### 4.4.3 責任

利用者は、本ポリシーの条項の不履行に起因する損害について、任意の当事者に対して責任を負う場 合がある。

## 5 ポリシーの管理

### 5.1 文書を管理する組織

Symantec Corporation
350 Ellis Street
Mountain View CA 94043
USA

### 5.2 連絡先情報

Symantec Validation and ID Protection (VIP) Network Product Manager
c/o Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
vip-practices@symantec.com

### 5.3 ポリシー変更手続

修正事項が重大でない（誤植の訂正、URL の変更、もとの意味を維持した用語の明確化、連絡先情報の 変更等）と Symantec が判断した場合に限り、本 VIP ポリシーは随時予告なく改訂されること

がある。Symantec は、Symantec レポジトリ（www.symauth.com/repository）の「Practices Updates and Notices」のページに改訂案を掲載する事で、重要な改訂案（全 VIP 参加者に重要な影響を及ぼす実質的な改訂等）に対するクレデンシャル発行者や依拠する当事者からのフィードバックやコメントを募集している。ポリシーの重大な改訂に対するコメント送付期間は、改訂案の掲載から 15 歴日とする。Symantec は、受信したすべてのフィードバックやコメントを検討し、以下のように対応する。（a）改訂案を修正なしで発効する、（b）改訂案にフィードバックを統合し、修正版を発効する、（c）改訂案を撤回する。改訂案の修正や撤回が ない場合、改訂案はコメント送付期間終了時に発効するものとする。改訂案は、参照したバージョンのポリシーの特定の条項や矛盾する条項に優先される。

# 6 用語集

| 用語 | 説明 |
|---|---|
| アクティベーション | 特定の依拠当事者が VIP クレデンシャルを有効化するプロセス。 |
| バインド | 依拠当事者が自ウェブサイトにおいて、アクティベートされた VIP クレデンシャルと、利用者のユーザ ID とを結びつけるプロセス。 |
| クレデンシャル発行者 | VIP クレデンシャルを発行する権限を持つ、VIP ネットワーク内の個人または組 織。 |
| クレデンシャルのライフサイクル管理機能 | VIP クレデンシャルのライフサイクルに関連する主要な管理機能。アクティベーション/ディアクティベーション、ロック/ロック解除、無効化/有効化、ワンタイムパスワードのみの VIP クレデンシャルの同期化などがある。 |
| デバイス | VIP クレデンシャルを保護するハードウェアデバイスやソフトウェアデバイス、または、VIP クレデンシャルが埋め込まれたハードウェアデバイスやソフトウェアデバイスで、ネットワークオペレータが VIP ネットワークでの使用を許可したもの。 |
| 無効化 | VIP クレデンシャルのステータスを一時的に[Enabled]から変更して、特定の依 拠当事者で使用できないようにすること。 |
| 有効化 | 無効化された VIP クレデンシャルのステータスを有効にし、無効化した依拠当 事者で使用できるように変更すること。 |
| 利用者 | VIP クレデンシャルを所有する、VIP クレデンシャルの個々の利用者。 |
| 停止 | 特定の依拠当事者が使用できないよう、有効化された VIP クレデンシャルのス テータスを[Inactive]に変更すること。 |
| ロック | 特定の依拠当事者が使用できないよう、VIP クレデンシャルのステータスを[Enabled]から変更すること。 |
| ネットワークオペレータ | VIP ネットワークのオペレータ。 |
| ワンタイムパスワード（OTP） | 暗号化アルゴリズムによって生成される使い捨てパスワード。利用者が所有する VIP クレデンシャルの検証に使用される。 |
| 依拠当事者 | 第 2 認証要素として、有効な VIP クレデンシャルを受入れる個人または組織。 |

| | |
|---|---|
| 共有鍵 | 利用者とネットワークオペレータのみが知っている、VIP クレデンシャルに関連付けられた、ランダムに生成されたコード。クレデンシャルの所有権を検証するために使用される。 |
| ロック解除 | ロックされた VIP クレデンシャルのステータスを[Enabled]にして、VIP ネットワークで特定の依拠当事者で使用できるように変更すること。 |
| Symantec アイデンティティプロテクションセンター | Symantec がクレデンシャル発行サービスを提供するウェブサイト。（https://idprotect.verisign.com） |
| VIP クレデンシャル | ワンタイムパスワードを生成する装置またはソフトウェア。 |
| VIP ネットワーク | Symantec VIP オーセンティケーションネットワークポリシーが適用される二要素認証ベースのインフラストラクチャ。VIP クレデンシャルの導入が可能であり、ネットワークオペレータ、クレデンシャル発行者、依拠当事者、利用者が VIP クレデンシャルを使用できるネットワーク。 |
| VIP 参加者 | VIP ネットワーク内で、ネットワークオペレータ、クレデンシャル発行者、依拠当 事者、利用者のうち、1 つまたは複数の役割を担う個人または組織。 |