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ございます。お客様を何ら拘束するものではありません。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ありません。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。

Copyright ©2013 Symantec Corporation. All rights reserved.  Symantec と Symantec ロゴは、Symantec Corporation または関連会社の米国およびその他の国における登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

The Symantec logo and Symantec Validation and ID Protection Service Network are trademarks and service marks of Symantec Corporation. Other trademarks and service marks in this document are the property of their respective owners. Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means （electronic, mechanical, photocopying, recording, or otherwise）, without prior written permission of Symantec Corporation.
Notwithstanding the above, permission is granted to reproduce and distribute these Symantec Validation and ID Protection （VIP） Service Network Policies on a nonexclusive, royalty-free basis, provided that （i） the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and （ii） this document is accurately reproduced in full, complete with attribution of the document to Symantec Corporation.
Requests for any other permission to reproduce these Symantec Validation and ID Protection Network Policies （as well as requests for copies from Symantec） must be addressed to Symantec Corporation., 350 Ellis Street, Mountain View, CA 94043 USA Attn: Symantec VIP Network Product Manager. Tel: +1 650.527.8000 Fax: +1 650.527.8050 E-mail:VIP-practices@symantec.com.
1 はじめに .................................................................................................................. 5

2 VIP ネットワーク参加者と相関関係 ......................................................................... 5
  2.1 VIP ネットワーク参加者 .................................................................................. 5
     2.1.1 ネットワークオペレータ ........................................................................... 5
     2.1.2 依拠当事者 ................................................................................................. 5
     2.1.3 クレデンシャル発行者 ................................................................................ 6
     2.1.4 利用者 ......................................................................................................... 6
  2.2 VIP 参加者の相関関係 ...................................................................................... 6

3 VIP クレデンシャル .................................................................................................. 7
  3.1 VIP クレデンシャル ......................................................................................... 7
  3.2 VIP クレデンシャルの所持証明 ...................................................................... 8
  3.3 VIP クレデンシャルのプロビジョニングおよび保護 ......................................... 8
     3.3.1 VIP クレデンシャルのプロビジョニング .................................................... 8
     3.3.2 VIP クレデンシャルの保護 ....................................................................... 8
  3.4 クレデンシャルのステータス ............................................................................ 9
  3.5 クレデンシャルの検証プロセス ...................................................................... 10
  3.6 クレデンシャルのライフサイクル管理 ............................................................... 10
     3.6.1 アクティベーション ..................................................................................... 11
     3.6.2 ロック/ロック解除 ................................................................................... 11
     3.6.3 無効化/有効化 ........................................................................................... 12
     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 ..................... 13
     3.6.5 VIP クレデンシャルの停止 ...................................................................... 13
     3.6.6 VIP クレデンシャルの失効 ..................................................................... 14

4 役割と責任 .................................................................................................................. 15
  4.1 ネットワークオペレータ .................................................................................. 15
     4.1.1 セキュリティ要件 ....................................................................................... 15
     4.1.2 運用要件 ..................................................................................................... 15
     4.1.3 プライバシー要件 ..................................................................................... 16
     4.1.4 責任 ............................................................................................................ 16
  4.2 依拠当事者 ......................................................................................................... 16
     4.2.1 セキュリティ要件 ....................................................................................... 16
     4.2.2 運用要件 ..................................................................................................... 17
     4.2.3 プライバシー ............................................................................................... 18
     4.2.4 責任 ............................................................................................................ 18
  4.3 クレデンシャル発行者 ...................................................................................... 18
4.3.1 セキュリティ要件..................................................................................................................19
4.3.2 運用要件.................................................................................................................................19
4.3.3 プライバシー要件.....................................................................................................................19
4.3.4 責任...........................................................................................................................................19
4.4 利用者.........................................................................................................................................20
  4.4.1 セキュリティ要件.....................................................................................................................20
  4.4.2 利用者の義務..........................................................................................................................20
  4.4.3 責任.........................................................................................................................................20
5 ポリシーの管理.............................................................................................................................20
  5.1 文書を管理する組織....................................................................................................................20
  5.2 連絡先情報..................................................................................................................................20
  5.3 ポリシー変更手続.......................................................................................................................20
6 用語集..............................................................................................................................................21
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することとする。

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た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使用するよう負担を負わずとも、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するため、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、利用者からの要件があり次第、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、依拠当事者のローカルディレクトリを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ものは第 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）アクティブ化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。

Symantec Corporation, Version 2.1, September 7, 2011
依頼当事者は、（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。依頼当事者は、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頼当事者を兼ね、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参加者は依頼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参加者は依頼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頼当事者とともに、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

依頼当事者は、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、依頼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頼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。

![Diagram](image)

End user: 利用者
Credential Issuer: クレデンシャル発行者
Relying Party: 依頼当事者
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、依頼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: 依頼当事者は、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: 依頼当事者は、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、この依頼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。

利用者と依頼当事者の間で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す。VIPクレデンシャルのアクティベーションと、依頼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2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頼当事者に提示する。依頼当事者は、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頼当者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. デバイス製造業者は、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全する。

2. デバイス製造業者は、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全する。

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ッ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。

Symantec Corporation, Version 2.1, September 7, 2011
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。

<table>
<thead>
<tr>
<th>ステータス</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>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。</td>
</tr>
<tr>
<td>Enabled (Active)</td>
<td>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。</td>
</tr>
<tr>
<td>Inactive</td>
<td>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。</td>
</tr>
<tr>
<td>Locked</td>
<td>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。</td>
</tr>
<tr>
<td>Disabled</td>
<td>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。</td>
</tr>
</tbody>
</table>

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](image)

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。

<table>
<thead>
<tr>
<th>ステータス</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>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。</td>
</tr>
<tr>
<td>Revoked</td>
<td>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。</td>
</tr>
</tbody>
</table>

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グロセスを完了し、依拠当事者のウェブサイトにバインドすると、その依拠当事者ウェブサイトは、要求認証のために、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
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。

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 クレデンシャルを発行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 クレデンシャルを証認、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、自身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じて 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じて 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不可である。

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 回を超えないことが推奨される。

Symantec Corporation, Version 2.1, September 7, 2011
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けた後、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。

- 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。
- 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。
- 利用者がVIP クレデンシャルの危険の懸念を報告し、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
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、特定の依頼当事者に関して VIP クレデンシャルを無効化可能である。各依頼当事者は、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、そ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頼当事者に要求可能である。ネットワークオペレータは、依頼当事者から VIP クレデンシャルの再有効化要求を受信した場合のみ、その依頼当事者に関して VIP クレデンシャルの再有効化可能である。依頼当事者は、(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 クレデンシャルにて生成される場合や、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

責任者利用者が再同期化要求を受けた際、該当する依頼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。依頼当事者が、(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、特定の依頼当事者に関して、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。その依頼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

特定の依頼当事者に関して、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。
- 利用者が依頼当事者との関係を終了したとき。
- 利用者が依頼当事者に関して 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。

Symantec Corporation, Version 2.1, September 7, 2011

13
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険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頼当事者に関する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、その依頼当事者に要求可能である。
依頼当事者は、停止要求が本ポリシーの条項で保証されている場合、VIPネットワーク上でその依頼当事者に対して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V.I.P.クレデンシャルのアクティペーションを担当した依頼当事者は、VIPネットワーク上でその依頼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V.I.P.クレデンシャルを停止可能である。各依頼当事者は、本ポリシー第4.2.2.1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。いかなる依頼当事者も、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。
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険が発生したとき。
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。
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、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とする。ペリサインは毎年、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 ネットワークの運用

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。

Symantec Corporation, Version 2.1, September 7, 2011
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を、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。
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以 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に、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出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致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を Symantec にセキュアに送付し、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）自らがアクトイ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は、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、第一交代支持を提供する。
- 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け入れるものとする。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。

Symantec Corporation, Version 2.1, September 7, 2011
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）

これらの場合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 日経過後は新しい一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ビ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、個人情報として取扱わず、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、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。

Symantec Corporation, Version 2.1, September 7, 2011
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ログ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ログを表示する。
- 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ログを表示する。

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有、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、データベース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じ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。

Symantec Corporation, Version 2.1, September 7, 2011
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者である。

4.4.1 セキュリティ要件

利用者は自己の V I P 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、その他の危険が発生した場合、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ブ化時に、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
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っている。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営業日とする。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

<table>
<thead>
<tr>
<th>用語</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>アクティベーション</td>
<td>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。</td>
</tr>
<tr>
<td>バインド</td>
<td>依拠当事者が自ウェブサイトにおいて、アクティベーション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。</td>
</tr>
<tr>
<td>クレデンシャル発行者</td>
<td>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。</td>
</tr>
<tr>
<td>クレデンシャルのライフサイクル管理機能</td>
<td>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VIPクレデンシャルの同期化などがある。</td>
</tr>
<tr>
<td>デバイス</td>
<td>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。</td>
</tr>
<tr>
<td>無効化</td>
<td>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。</td>
</tr>
<tr>
<td>有効化</td>
<td>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。</td>
</tr>
<tr>
<td>利用者</td>
<td>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。</td>
</tr>
<tr>
<td>停止</td>
<td>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。</td>
</tr>
<tr>
<td>ロック</td>
<td>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。</td>
</tr>
<tr>
<td>ネットワークオペレータ</td>
<td>VIPネットワークのオペレータ。</td>
</tr>
<tr>
<td>ワンタイムパスワード（OTP）</td>
<td>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。</td>
</tr>
<tr>
<td>依拠当事者</td>
<td>第2認証要素として、有効なVIPクレデンシャルを受け入れる個人または組織。</td>
</tr>
</tbody>
</table>
### 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。