Tor の安全な使用方法について
（DNS Leakage の観点から）

ＮＴＴ コミュニケーションズ株式会社
経営企画部
マネージドセキュリティサービス推進室
セキュリティオペレーション担当

2013 年 03 月 13 日

Ver. 1.0

1. 調査概要 3
1.1. 調査概要 3
2. 注意事項 3
3. DNS LEAKAGE以外の問題について 3
4. WEBブラウザのSOCKS実装状況について 4
4.1. TOR BROWSER BUNDLE 2.3.25-4 の場合 4
5. SOCKSとTORと名前解決 6
5.1. Torを使った場合のDNSからのクライアントIPアドレスの漏洩 6
5.2. TorとDNS LEAKAGE 6
6. 安全なTORの使用方法 8
6.1. TOR BROWSERバンドル(TOR BROWSER)の使用 8
7. 現時点では好ましくないTORの使用方法 11
7.1. POLIPO (SOCKSへ転送可能なHTTPプロキシ) の利用 11
7.2. GOOGLE CHROMEの使用 12
7.3. WEBブラウザのSOCKS機能を使う 12
8. その他、TORの利用について 12
8.1. Torノードとして起ち上げる際の注意点 (EXITリレー) 12
8.2. その他(日本語化) 14
9. 検証作業者 16
10. 履歴 16
11. 最新版の公開URL 16
12. 参考 16
13. 本レポートに関する問合せ先 17

1. 調査概要

1.1. 調査概要

Web ブラウザの SOCKS プロキシ機能の実装状況の調査によって Web ブラウザの SOCKS プロキシ機能には、DNS Leakage の問題があることが確認された。よって、クライアントのプライバシーを保護する Tor を Web ブラウザ経由で利用する場合、普段使っている Web ブラウザを使わずに、Tor Project から提供されているプライバシー保護のためにチューニングされている Tor Browser Bundle の Web ブラウザ(Tor Browser)を使用することを強く推奨する。
どうしても、普段使っている Web ブラウザを使う必要がある場合(そのような現実的な場面を想定できないが)、以前に Tor にバンドルされている polipo(そのまた以前は privoxy だった)などの SOCKS へ転送可能な HTTP プロキシを経由させることなども考えられるが、現在では推奨されない。

参考
- 「Web ブラウザの SOCKS 実装状況について」
  http://www.ntt.com/icto/security/data/soc.html

2. 注意事項

Tor は元々、言論の自由のない弾圧された国家や社会などで暮らす人々へ匿名でも発言できるように、また(国家権力の犯罪行為など)巨悪を告発する際の告発者のプライバシーを保護するために作られたもので、犯罪者が身元を隠すためのツールではない。
当然だが、本文書の内容を悪用することは厳禁とする。
本文書の内容が、言論の自由を奪われ弾圧されている人々の役に立てれば、個人的に幸いである。

3. DNS Leakage以外の問題について

本文書では、DNS Leakage に注目しているが、DNS Leakage 以外にも、Web ブラウザ上のプラグインやスクリプトなどから漏洩する問題などもあるが、それらは本文書の扱う範囲外とする。

4. WebブラウザのSOCKS実装状況について

以下を参照のこと

- 「Web ブラウザの SOCKS 実装状況について」
  http://www.ntt.com/icto/security/data/soc.html

既定の設定で利用する限り、ほとんどの Web ブラウザには、DNS Leakage の問題が残っているため、プライバシー保護が必要な場面で、普段利用している Web ブラウザを使うのは危険が伴うといえる。

4.1. Tor Browser Bundle 2.3.25-4 の場合

Tor Browser Bundle では、Tor にプライバシー保護のためにチューニングされた Web ブラウザが同梱されている。その Web ブラウザ(Firefox の英語版)を使用したところホスト名を IP アドレスへ変換するための名前解決を自ら行うようなことなかった。

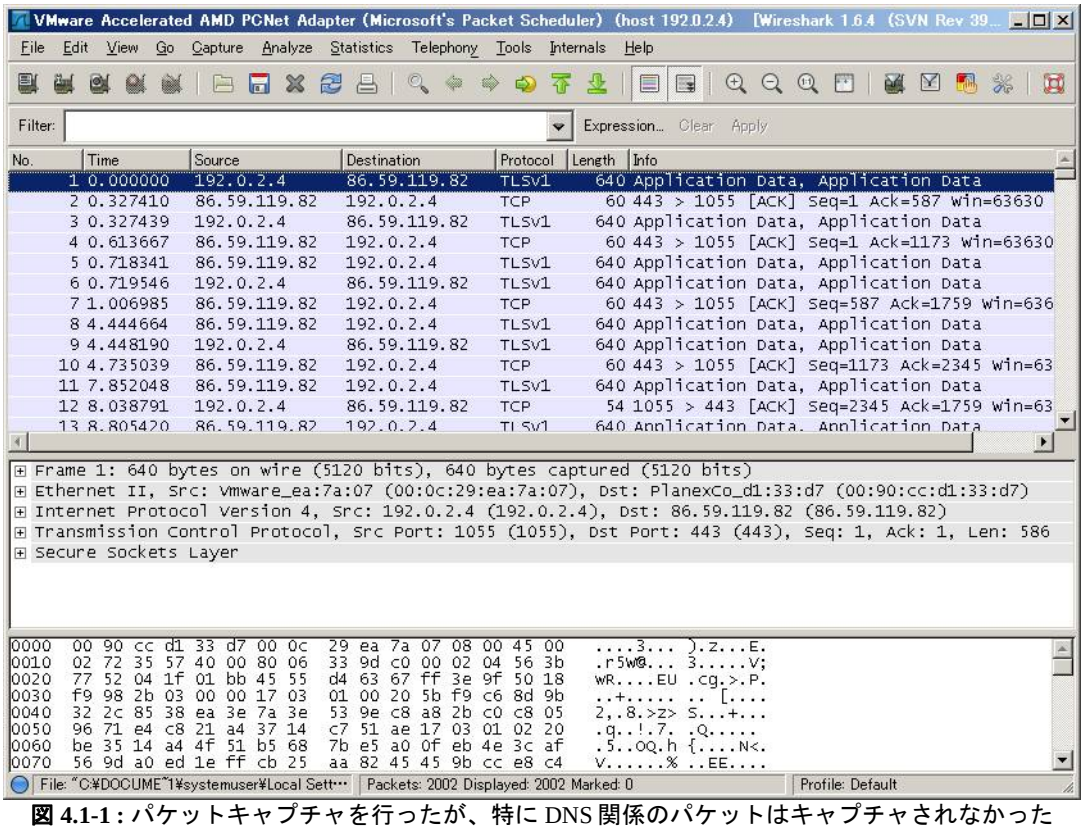

図 4.1-1 : パケットキャプチャを行ったが、特に DNS 関係のパケットはキャプチャされなかった

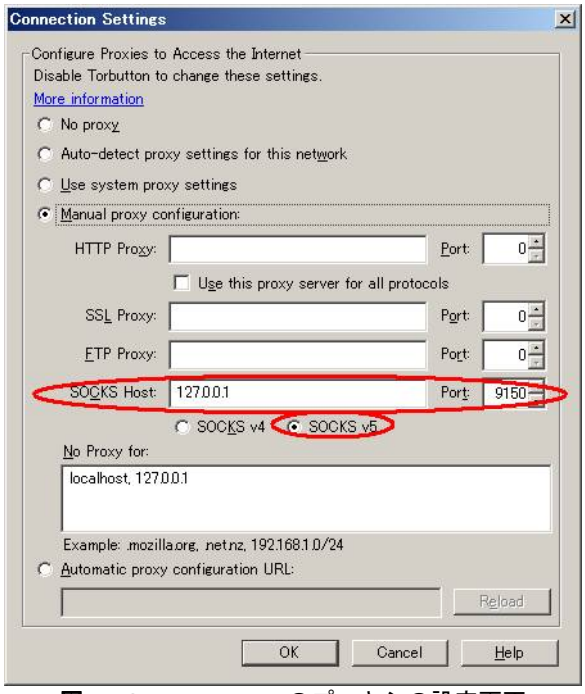

図 4.1-2 : Tor Browser のプロキシの設定画面

通常の Tor とバッテングしないように!?ポート番号が「9150/tcp」になっている

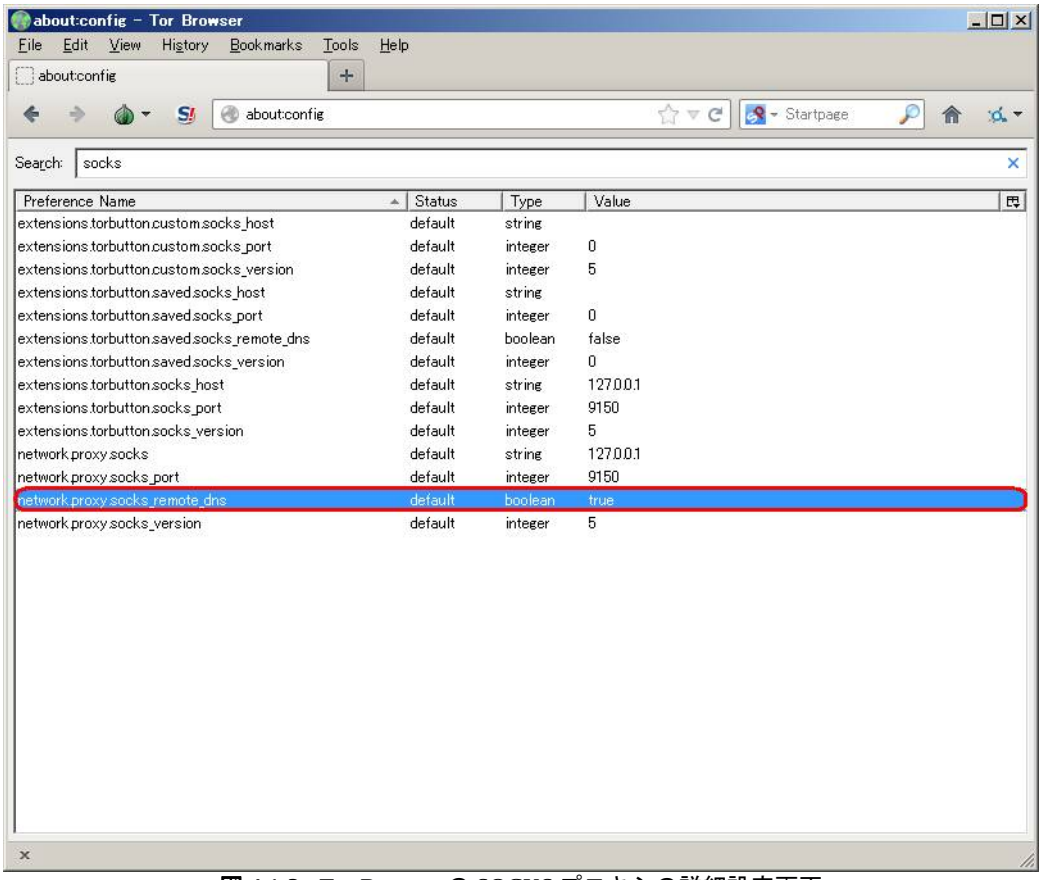

図 4.1-3 : Tor Browser の SOCKS プロキシの詳細設定画面

「network.proxy.socks_remote_dns=true」となっている

5. SOCKSとTorと名前解決

5.1. Torを使った場合のDNSからのクライアントIPアドレスの漏洩

Tor は、クライアントの IP アドレスを隠蔽し、プライバシーを保護するソフトウェア/ネットワーク/システムである。Tor は SOCKS サーバとして稼動しているため、SOCKS を入り口として、Tor ネットワークを使って通信することができる。

もし、クライアントが実装している SOCKS 自体が version4 の場合、通信を行うクライアント・ソフトウェア自体が DNS 解決を行う必要があるため、クライアントの IP アドレスが、DNS サーバ側のログとして残る可能性がある(DNS Leakage)。
また、Web ブラウザの SOCKS 実装の状況から、ほとんどの Web ブラウザ(の既定の設定)には、DNS Leakage の問題が残っている。たとえ、SOCKSv4a や SOCKSv5 が実装されている場合でも、Web ブラウザが自ら名前解決を行っている場合があるからである。

5.2. TorとDNS Leakage

DNS サーバに対して、クライアント IP アドレスが漏洩したとしても、DNS の仕組み上、一般的には、クライアントに一番近い DNS サーバに対しての漏洩となり、サーバ側で管理している DNS サーバまで情報が漏洩するわけではない。また、DNS Leakage を使ってクライアントを特定するには、DNS キャッシュの仕組みや、ISP 側から提供されている DNS サーバや、それによる再帰的問い合わせ、さらにはインターネット上に点在する公開 DNS サーバなど、DNS の仕組みを考慮すると、かなりの困難が予想される。

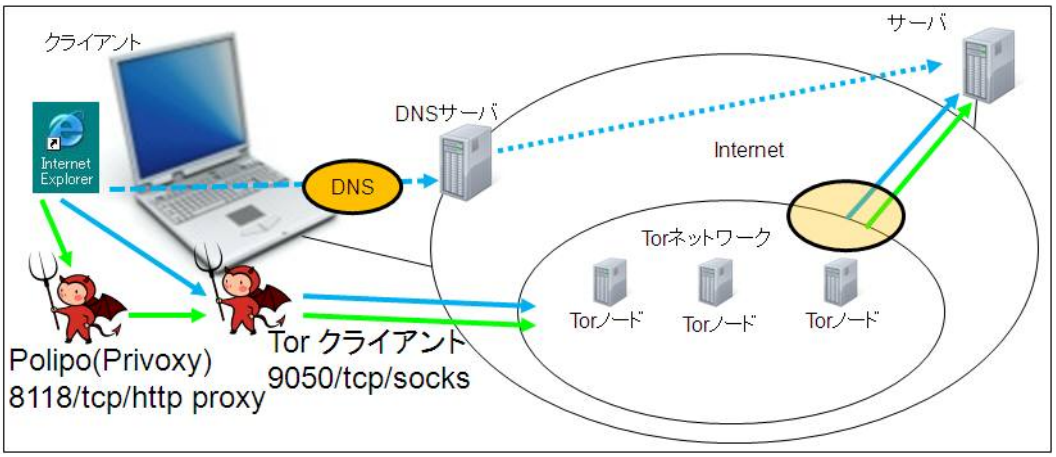

図 5.2-1 : Tor といろいろなツールとの関係

クライアントが SOCKSv4 のみ対応の場合、

DNS サーバにクライアント側 IP アドレスがログとして残る可能性がある

実際には、ほとんどの Web ブラウザが自ら名前解決を行ってしまい、DNS Leakage の危険性がある

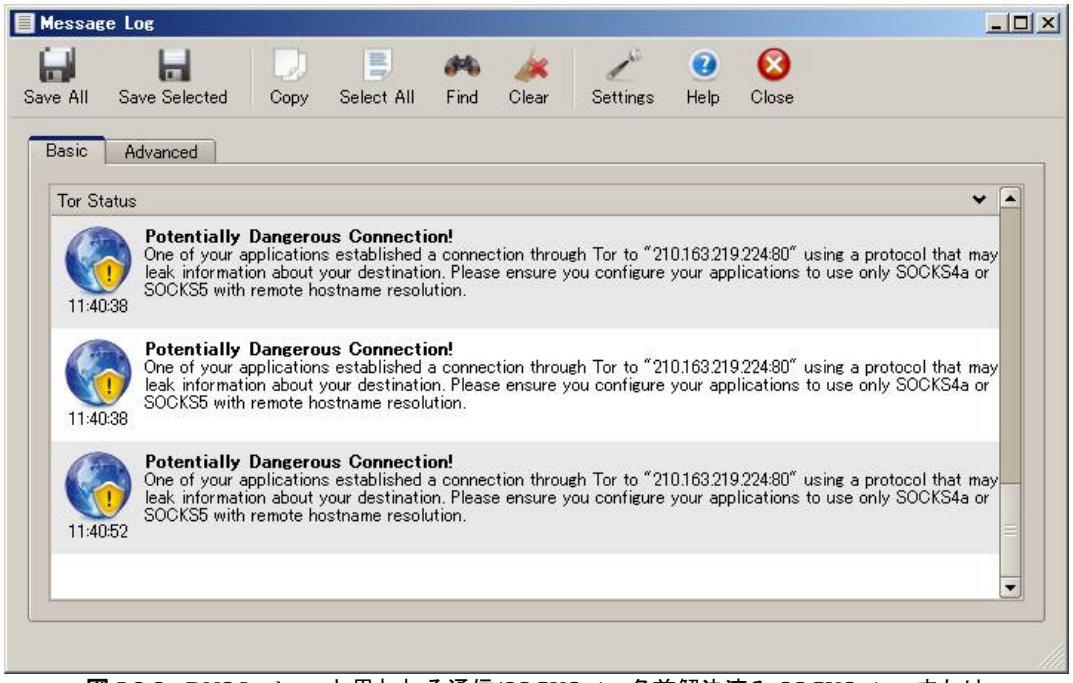

図 5.2-2 : DNS Leakage と思われる通信(SOCKSv4、名前解決済み SOCKSv4a、または名前解決済み SOCKSv5)をクライアント側から行うと、Tor 側に警告ログが表示される

6. 安全なTorの使用方法

6.1. Tor Browserバンドル(Tor Browser)の使用

Tor Project が提供している Web ブラウザがバンドルされた Tor を使用することを強く推奨する。
Tor Browser には、DNS Leakage 以外の問題についても対策されている。
重ねて、Tor Browser の使用を強く推奨する。

また、念のため、MS-Windows の「DNS Client」サービスを停止しておいてもよいかもしれない。

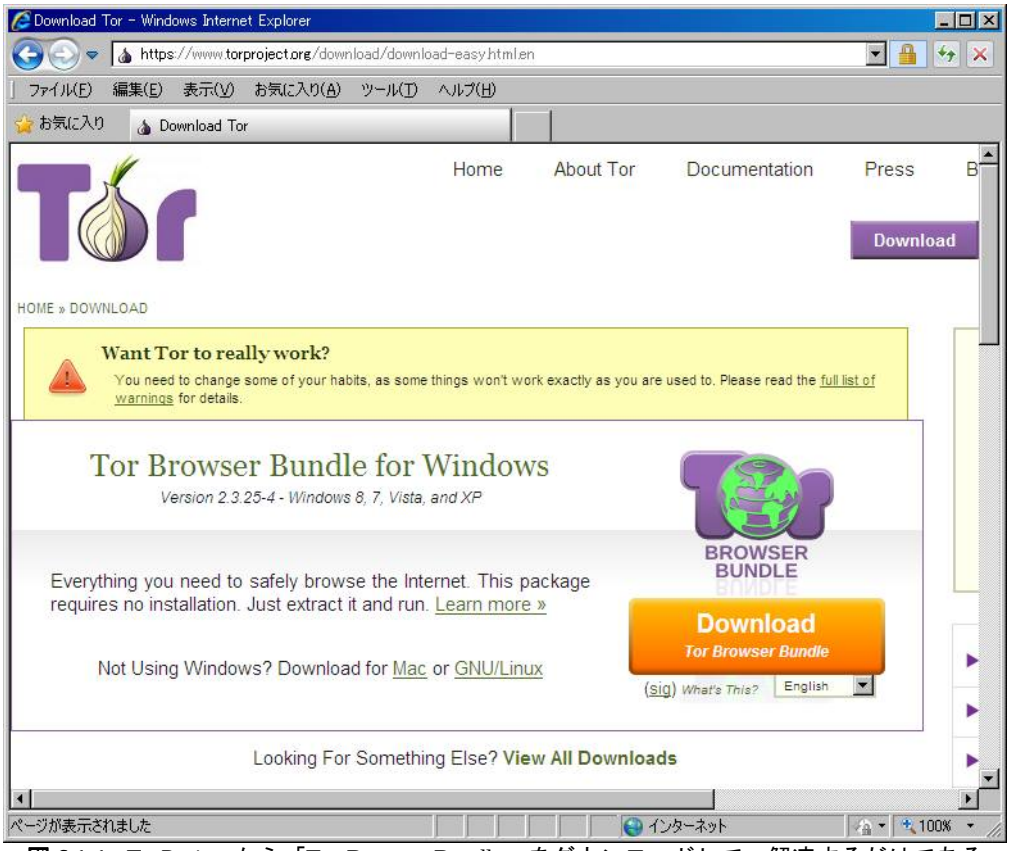

図 6.1-1 : TorProject から「Tor Browser Bundle」をダウンロードして、解凍するだけである

図 6.1-2 : TorProject から「TorBrowser」をダウンロードして、解凍するだけである

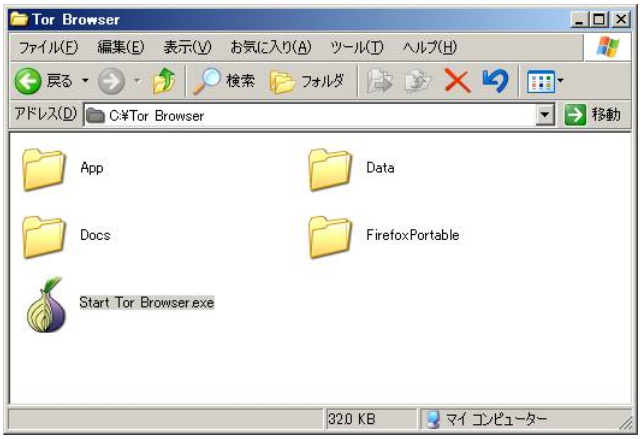

図 6.1-3 : 図 6.1-2を解凍してできたフォルダ。起動するだけである

(場合によってはこのフォルダをUSBメモリに入れて持ち歩く事も可能だ)

(MS-WindowsにはどのUSB機器を接続したかどうかの履歴が残ることに注意)

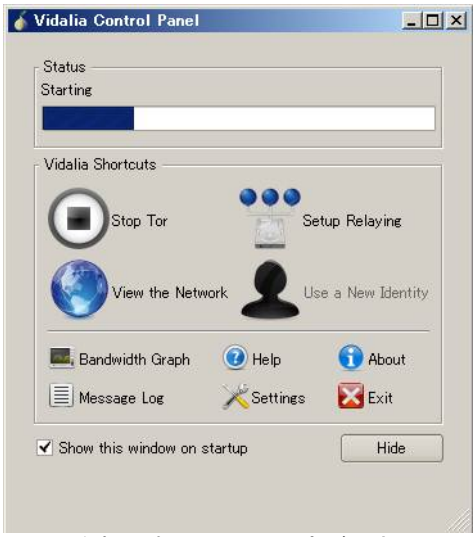

図 6.1-4 : 図 6.1-3を起動するとTorの設定ができるGUIが起動する

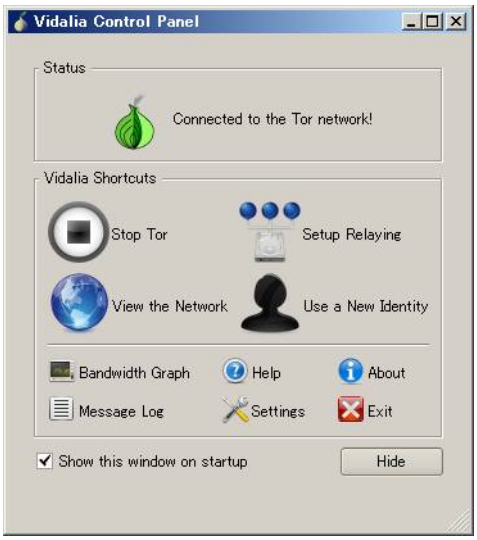

図 6.1-5 : 図 6.1-4後、Torネットワークへの接続が完了すると、

チューニングされたFirefoxが起動しはじめる

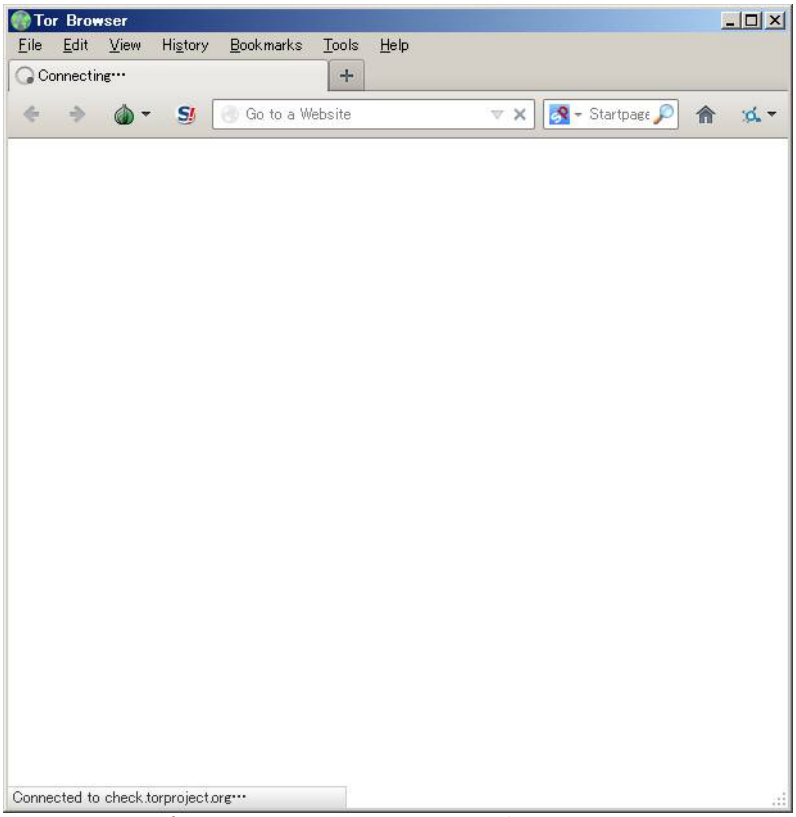

図 6.1-6：図 6.1-5後、プライバシー保護にチューニングされた英語版のFirefoxが起動する

7. 現時点では好ましくないTorの使用方法

実際にプライバシー保護が必要とする場面では、Tor Browser の使用が強く推奨される。
以下の方法は、2013 年時点では、推奨されない方法である。

7.1. polipo (SOCKSへ転送可能なHTTPプロキシ) の利用

Tor Browser を利用できない場合、以前の Tor にバンドルされているローカル HTTP Proxy サーバの「polipo」の併用する方法もある。
ただし、最新バージョンでは、Tor をクライアントとして利用する際の Tor Browser 以外のパッケージが提供されていないなど、現実的な方法ではない。
また、経由することになる SOCKS へ転送可能な HTTP プロキシサーバ(polipo については、Web ブラウザの SOCKS 実装調査時に調査済)の DNS Leakage については、調査しておく必要があるだろう。

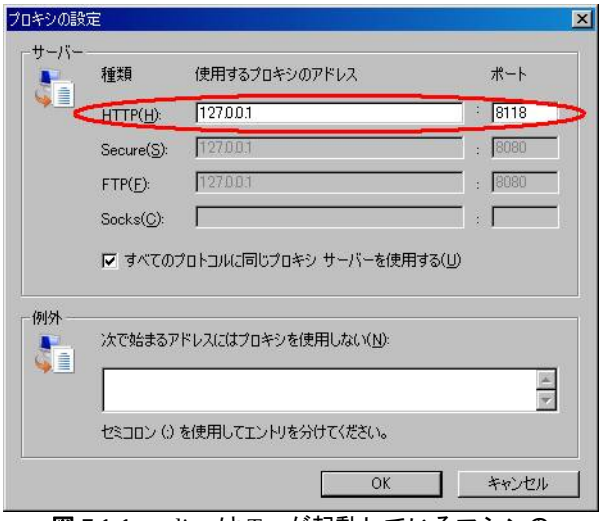

図 7.1-1 : polipo は Tor が起動しているマシンの
「8118/tcp」に HTTP Proxy として待ち受けしている

参考:

- 「Web ブラウザの SOCKS 実装状況について」
  http://www.ntt.com/icto/security/data/soc.html

7.2. Google Chromeの使用

参考 URL にあげているが、かつて Google Crome は大量の DNS リクエストを発生する場合があったようだ。
アドレス欄で Web ページを検索するはずが、DNS へ検索クエリーを投げているかもしれない。
DNS Leakage の可能性がでてくるため、Tor を使う上ではあまり好ましくないだろう。

参考:
- 極楽せきゅあ日記 [その他]自重しろ？＞クロム
  http://d.hatena.ne.jp/sonodam/20081104/p1

7.3. WebブラウザのSOCKS機能を使う

ほとんどの Web ブラウザ(※)で、SOCKS 機能には、DNS Leakage の問題が残っている。

(※)： Firefox の詳細設定を変更した状態と Safari では、DNS Leakage は確認されなかったが、例外的であり、基本的に普段使用する「Web ブラウザ+Tor」という組み合わせでプライバシー保護はおすすめできない。

参考
- 「Web ブラウザの SOCKS 実装状況について」
  http://www.ntt.com/icto/security/data/soc.html

8. その他、Torの利用について

8.1. Torノードとして起ち上げる際の注意点 (Exitリレー)

本章では、Tor ノードを立ち上げる際の注意点を挙げる。

Tor ノードとして参加する場合、以下の形態がある。
- Exit リレー：Tor ネットワークの最終経路となることもいとわないで参加する形態
- Non-Exit リレー：最終経路はごめんだが、Tor ノードとして参加する形態
- Bridge：Tor への入り口を監視されている利用者向けに提供される “隠された” 入り口として参加する形態

上記の Tor ノードとして参加する種類の中でも「Exit リレー」については注意する必要がある。
- Exit ノードは自ら(Tor ノードを立ち上げているコンピュータ)の IP アドレスがサーバ側に通知される。
  弁護士や、人権擁護団体などとは異なり、法的保護がしっかりしていない利用者は、Exit リレーとして参加しない方が無難だろう。

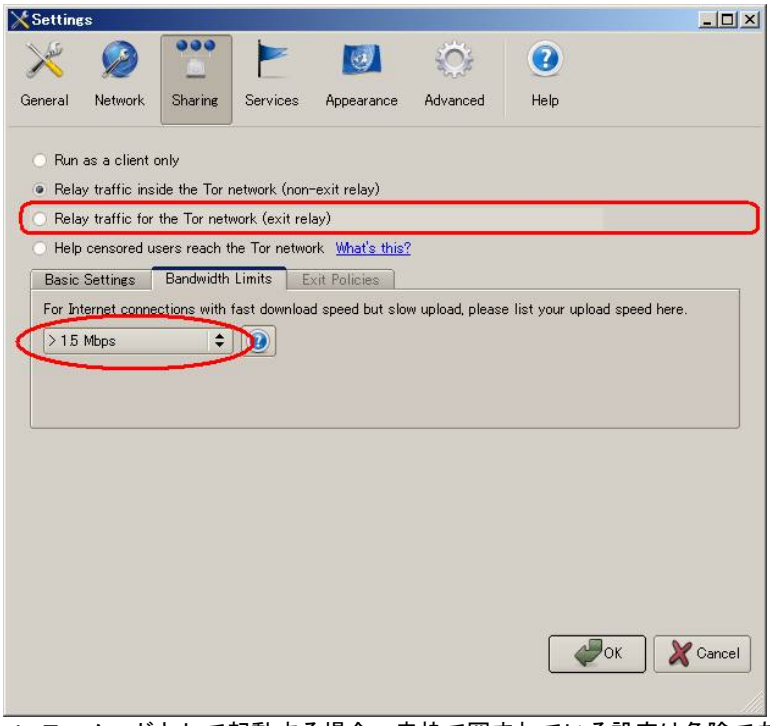

図 8.1-1 : Tor ノードとして起動する場合、赤枠で囲まれている設定は危険である。
「Exit node」になる可能性があり、それは Tor 利用者に成り代わって IP アドレス
をサーバ側に通知することを意味している

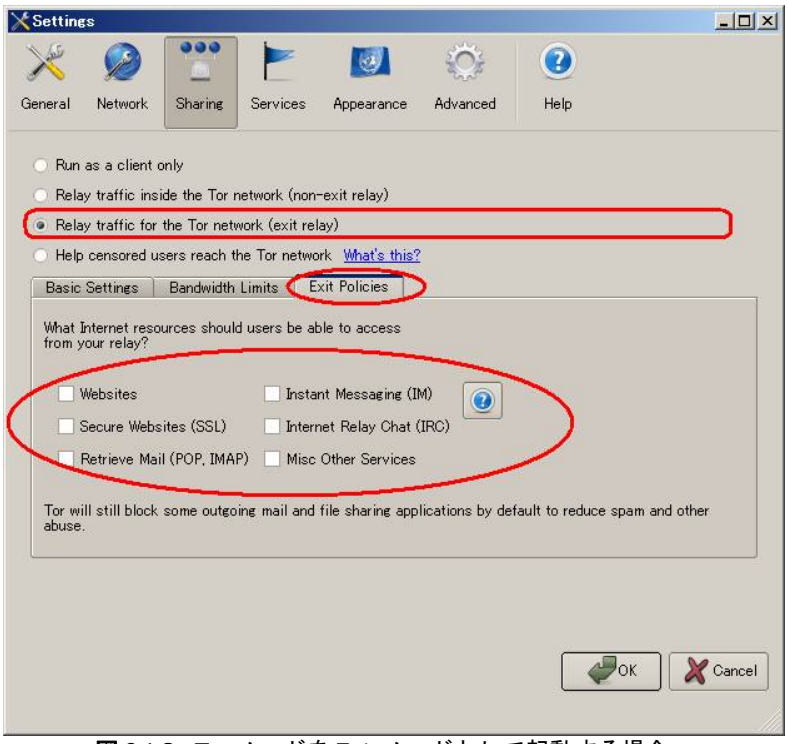

図 8.1-2 : Tor ノードを Exit ノードとして起動する場合、
最低限「Exit Policies」については入念に検討したほうがよいだろう
例えば、Web だけ提供したいということであれば、
「"Websites" & "Secure Websites (SSL)"」だけチェックすればよい

8.2. その他(日本語化)

以前は、Tor をコントロールする Vidalia には「日本語」が設定可能であったが、翻訳者がいなくなったためなのか、最新バージョンでは設定することができない。
ボランティア可能な方は、日本語化に協力してみてはいかがだろうか。

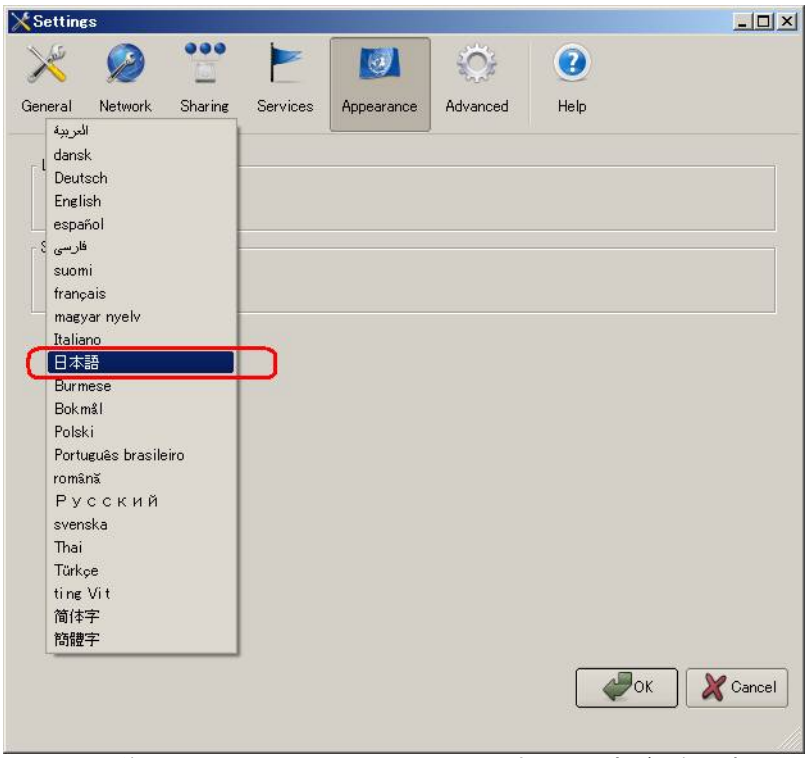

図 8.2-1：以前の Vidalia 0.2.12/Tor 0.2.1.30 **では日本語の設定が可能であった** 1

図 8.2-2：以前の Vidalia 0.2.12/Tor 0.2.1.30 **では日本語の設定が可能であった** 2

図 8.2-3 : 以前の Vidalia 0.2.12/Tor 0.2.1.30 では日本語の設定が可能であった 3

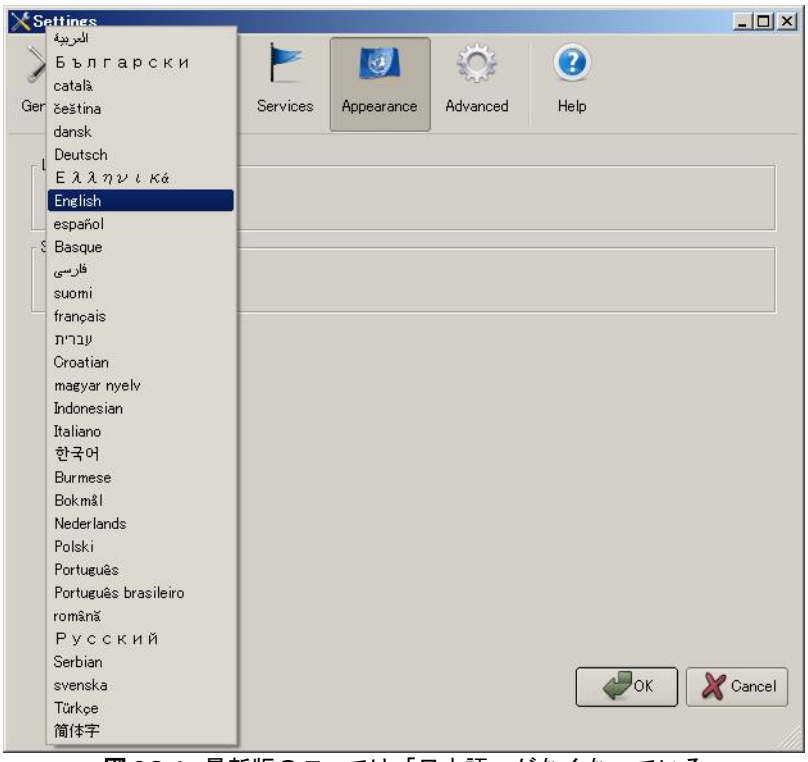

図 8.2-4 : 最新版の Tor では「日本語」がなくなっている

9. 検証作業者

NTT コミュニケーションズ株式会社
経営企画部マネージドセキュリティサービス推進室
セキュリティオペレーション担当
　佐名木 智貴

10. 履歴

- 2013 年 03 月 13 日 ：ver1.0 最初の公開

11. 最新版の公開URL

http://www.ntt.com/icto/security/data/soc.html

12. 参考

- 「Web ブラウザの SOCKS 実装状況について」
  http://www.ntt.com/icto/security/data/soc.html
- SOCKS
  http://ja.wikipedia.org/wiki/SOCKS
- SOCKS: A protocol for TCP proxy across firewalls
  http://ftp.icm.edu.pl/packages/socks/socks4/SOCKS4.protocol
- RFC1928
  http://tools.ietf.org/html/rfc1928
- RFC1929
  http://tools.ietf.org/html/rfc1929
- RFC1961
  http://tools.ietf.org/html/rfc1961
- Tor Project
  https://www.torproject.org/
- 極楽せきゅあ日記 [その他]自重しろ？ ＞クロム
  http://d.hatena.ne.jp/sonodam/20081104/p1

13. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
経営企画部
マネージドセキュリティサービス推進室
セキュリティオペレーション担当

e-mail: scan@ntt.com

以 上