

Trusteer Rapport ユーザーガイド

バージョン3.5.1207

2012年10月

new threats, new thinking

新たな脅威、新たな考え方

目次

本書について	1
Trusteer Rapportの詳細情報について	1
弊社へのフィードバック	2
1. 新機能について	3
2. Trusteer Rapportについて	5
概要	5
危機にさらされているもの	7
Trusteer Rapportが必要とされる理由	8
Trusteer Rapportで保護できる攻撃	10
フィッシング	11
ファージングまたはDNS偽装	12
キーロギング	12
中間者攻撃	13
マンインザブラウザ攻撃	13
スクリーンキャプチャー	14
セッションハイジャック	14
自動ダウンロード	15
Trusteer Rapportの動作原理	15
保護されたサイトとの安全な通信	17
ログイン保護	17

ブラウジングセッション保護	18
キーストローク保護	18
クレジットカード保護	19
スクリーンキャプチャーのブロック	19
Webサイト検証	19
ブラウザーアドオンのブロック	20
プロセス変更のブロック	20
悪意のあるWebサイトの警告	20
不正アクセスのレポート	21
ユーザーエクスペリエンス	21
Trusteer Rapportの有効活用	22
高度なユーザーのための情報	23
Trusteer RapportのPCフットプリント	23
Trusteer Rapportとお客様のプライバシー	24
Trusteer Rapportセントラルサービス: 強力な詐欺行為ブロック機能	24
3. Trusteer Rapportのインストール	27
Internet Explorerを使用したWindows 7へのTrusteer Rapportのインストール	31
Internet Explorerを使用したWindows XPへのTrusteer Rapportのインストール	36
Firefoxを使用したWindows 7へのTrusteer Rapportのインストール	42
Google Chromeを使用したWindows 7へのTrusteer Rapportのインストール	49

Firefoxを使用したWindows XPへのTrusteer Rapportのインストール	55
Google Chromeを使用したWindows XPへのTrusteer Rapportのインストール	61
Windows Server (2003または2008)へのTrusteer Rapportのインストール	67
4. アプリケーションの開始	69
追加のWebサイト保護	70
Rapportコンソールのオープン	72
5. オンラインバンキングの保護	75
6. 企業Webサイトの保護	76
7. オンラインでの安全なクレジットカードの使用	77
8. Trusteer Rapportの仮想化ブラウザの使用	79
9. Trusteer Rapportのセキュアソフトトークンの使用	83
セキュアソフトトークンの有効化	83
OTPの生成	87
OTPアカウントの管理	88
<i>OTPアカウントの名称変更</i>	89
<i>OTPアカウントの削除</i>	90
10. アラートおよび警告への応答	92
仮想化ブラウザの強制ダウンロードアラートに対する応答	92
仮想化ブラウザの強制アラートに対する応答	94
仮想化ブラウザのオプションダウンロードアラートに対する応答	95

仮想化ブラウザのオプションアラートに対する応答	101
パスワード保護の提示に対する応答	107
保護情報の警告に対する応答	117
安全でない送信の警告に対する応答	119
フィッシングサイトの警告に対する応答	124
感染したWebページの警告に対する応答	128
クレジットカード情報送信検知の警告に対する応答	129
クレジットカード保護のメッセージに対する応答	131
[プリントスクリーン検知]アラートに対する応答	132
ブラウザ保護アラートに対する応答	133
マルウェア駆除の有効化アラートに対する応答	137
マルウェア駆除の開始アラートに対する応答	138
アンインストール中のマルウェア感染アラートに対する応答	140
無効な証明書の警告への応答	141
アクティビティレポートの通知に対する応答	146
Trusteer Rapportのアップグレードのプロンプトに対する応答	147
コード更新の管理メッセージに対する応答	148
画面読み上げ互換モードの警告に対する応答	148
管理者モードからの再インストールアラートに対する応答	150
管理者アカウントへの切り替え(Windows 7)	152
管理者アカウントへの切り替え(XP)	154
管理者アカウントへの切り替え(Vista)	156

<i>Trusteer Rapport のアンインストール(Windows 7)</i>	157
<i>Trusteer Rapport のアンインストール(Windows XP)</i>	158
<i>再起動を求めるアラートに対する応答</i>	159
11. Trusteer Rapportのカスタマイズ	160
<i>Trusteer Rapportのアドレスバーアイコンの表示/非表示</i>	160
<i>システムトレイアイコンの表示/非表示</i>	162
<i>インターフェース言語の変更</i>	163
12. Trusteer Rapportのアクティビティの表示	166
<i>アクティビティレポートの表示</i>	166
<i>アクティビティレポートの設定</i>	168
13. セキュリティ向上のためのコンピューターのスキャン	170
<i>手動スキャンの実行</i>	170
<i>セキュリティ上のベストプラクティスレポートの表示</i>	171
14. セキュリティニュースの受信	175
<i>セキュリティニュースセンターの表示</i>	176
<i>セキュリティニュースチャンネルの購読</i>	178
<i>通知の購読</i>	179
15. 保護されたサイトおよびパスワードの管理	181
<i>保護されたWebサイトの管理</i>	181
<i>保護されたユーザー名およびパスワードの管理</i>	184
16. Trusteer Rapportのセキュリティポリシーの変更	187

セキュリティポリシーサマリーの表示	187
セキュリティコントロールの変更	189
セキュリティポリシーコントロールについて	194
17. トラブルシューティング	207
Trusteer Rapportの停止	207
Trusteer Rapportの起動	209
サポートについて	210
正規ブラウザアドオンのブロック解除	210
キーロガーブロック機能の無効化	213
誤った承認の取り消し	216
エラーへの対応	227
プロキシサーバーの自動更新の設定	231
ユーザー問題レポートの送信	234
TrusteerへのTrusteer Rapportログファイルの送信	236
18. Trusteer Rapportの最新状態の維持	241
Trusteer Rapportの更新ステータスのチェック	241
Rapportの手動更新	243
自動更新の無効化	245
19. Trusteer Rapportのアンインストール	249
Trusteer Rapport のアンインストール(Windows 7)	251
Trusteer Rapport のアンインストール(Windows XP)	252

本書について

本書は、Trusteer Rapportの使用方法および製品を最大限に有効活用する方法について説明します。本書の対象となる読者は、以下のとおりです。

- 金融口座のオンライン使用を保護するためのセキュリティツールとして、Trusteer Rapportを無償ダウンロードで提供している銀行またはその他の金融機関のお客様
- Trusteer Rapportを使用して、会社へのリモートWebアクセスのセキュリティを確保している企業の社員の方
- Trusteer Rapportを使用して、オンラインでのクレジットカードのトランザクションのセキュリティを確保している、Trusteer Rapportで保護されたクレジットカードをご利用のお客様

Trusteer Rapportの詳細情報について

本書の補足情報として、TrusteerはすべてのFAQ (よく寄せられる質問)をWebページ(<http://www.trusteer.com/support/faq>)で提供しています。

FAQ Webページでは、nanoRepの提供するサービスにより、追加のご質問に対する答えを素早く見つけることができます。

素早く回答を探すには:

質問をここに入力し、以下に表示される回答を参照してください。

ご質問内容を入力するだけで、nanoRepにより回答が表示されます。


弊社へのフィードバック

Trusteerはお客様からのフィードバックを重視しています。

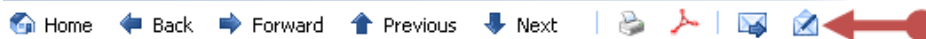
- Trusteer Rapportに関する新しい機能や改善点のご提案、およびご意見をお寄せください。

Trusteer Rapportについてのフィードバックは、以下のページからお送りください。<http://www.trusteer.com/ja/support/product-feedback> _本書に関する新しいトピックや改善点のご提案、およびご意見をお寄せください。

➔ 本書に関するフィードバックの送信方法

Trusteer Rapportのユーザーガイドページ上部にある[フィードバックを送信]ボタン  をクリックしてください。このボタンをクリックすると、ご使用のデフォルトの電子メールクライアントが起動し、弊社へのフィードバックをお送りいただけます。

Rapport Version 3.5.1108 User Guide



フィードバック
ボタン

1. 新機能について

Trusteer Rapport 1207の新機能は、以下のとおりです。

- Trusteer Rapport 1207のWindows 8に対する互換性がテストされ、認定されました。

Trusteer Rapport 1206の新機能は、以下のとおりです。

- Trusteer Rapport 1206は、保護されたWebサイトに対して新たに追加されたアプリケーション保護レイヤーである、仮想化ブラウザを提供しています。仮想化ブラウザは、ご使用のコンピューターのWindows OS上の独自の仮想マシン内で実行されるブラウザです。Trusteerにより、ご使用のコンピューター上で深刻なセキュリティリスクが検知されるか、ユーザーが仮想化ブラウザをサポートしているサイトをブラウザすると、Trusteer Rapportにより、仮想化ブラウザでサイトを開くことが促されます。仮想化ブラウザは、アラートからダウンロードしてインストールします。ワンタイムインストールを実行した後は、ブラウザでサイトを開くオプションが提供されたときに、アラートが表示され、特定のWebサイトを自動的に仮想化ブラウザで開くように設定できます。仮想化ブラウザの情報については、以下を参照してください。

- [「Trusteer Rapportの仮想化ブラウザの使用」\(79ページ\)](#)
- [「仮想化ブラウザの強制ダウンロードアラートに対する応答」\(92ページ\)](#)
- [「仮想化ブラウザの強制アラートに対する応答」\(94ページ\)](#)
- [「仮想化ブラウザのオプションダウンロードアラートに対する応答」\(95ページ\)](#)
- [「仮想化ブラウザのオプションアラートに対する応答」\(101ページ\)](#)

- Trusteer Rapport 1206では、ワンタイムパスワードを割り当てるためのセキュアソフトトークンサービスが、パートナーに対して提供されています。Trusteer Rapportのセキュアソフトトークンサービスは、マルウェアによるワンタイムパスワードの自動生成や盗難に対する保護を提供します。銀行または会社からTrusteer Rapportのセキュアソフトトークンサービスを使用するように要求されているお客様は、[「Trusteer Rapportのセキュアソフトトークンの使用」](#) (83ページ)を参照してください。

2. Trusteer Rapport について

Trusteer Rapportは、銀行などの機密性の高いWebサイトや勤務先の企業のプライベートネットワークなどに接続する際に、ブラウザベースの詐欺行為からユーザーを保護することを目的として、特別に設計されたセキュリティソフトウェアアプリケーションです。Trusteer Rapportは、最も強力な認証およびアンチウィルスソリューションを回避し、ブラウザを悪用してオンラインの金融およびデータに関する詐欺行為を行うZeusなどのマルウェアから、ユーザーを保護します。

Trusteer Rapportは、自動ダウンロード、フィッシング、ファームिंग、キーロギング、中間者攻撃、マンインザブラウザ攻撃、悪意のあるスクリーンキャプチャー、およびセッションハイジャック攻撃などの、ブラウザで発生する各種攻撃からユーザーを保護します。

概要

今やWebブラウザは、皆様がオンラインで銀行取引や買い物を行う際や、会社にリモート接続する際に利用する通信チェーンにおいて、最も脆弱なリンクとなっています。アンチウィルス、ファイアウォール、およびその他のデスクトップセキュリティソフトウェアは、既知の動作のリストに基づいて、マルウェアを特定し、駆除します。最近の研究では、最先端のアンチウィルスソリューションを使用しているにもかかわらず、金融マルウェアイベントの検知率が極端に低くなっていることが指摘されています。ご使用のブラウザまたはオペレーティングシステムに、マルウェアが検知されずに埋め込まれてしまった場合、攻撃が発生した場合でも、これらのソリューションは悪意のあるアクティビティに対抗しません。

従業員、請負業者、および顧客にリモートアクセスを提供している企業の場合、VPN (仮想プライベートネットワーク)、トークン、NAC、およびその他の認証方法を使用して、ユーザーを識別し、機密性の高い企業または個人のデータを保護していたとしても、ブラウザーベースの攻撃には脆弱性を露呈しています。最近のマルウェアは、ブラウザーを攻撃することでこれらの認証テクノロジーを回避し、リモートアクセスセッションを攻撃して、ログイン認証情報やデータを盗んだり、ネットワーク上のホストを感染させたりしています。

Trusteer Rapport以外のセキュリティソリューションは悪意のあるソフトウェアの検出および無効化に重点を置っていますが、Trusteer Rapportは、攻撃ポイントに対抗するアプローチにより、ご使用のブラウザーを保護します。Trusteer Rapportには、マルウェアによるブラウザーを介した機密性の高い個人情報および金融情報へのアクセスを認識する、有効な手法が採用されています。Trusteer Rapportは、攻撃ポイントで悪意のある動作を検知することにより、新しいマルウェアの亜種を迅速かつ正確に特定できます。Trusteer Rapportは以下の3つの階層で構成されている保護を提供します。

- まだ認識されていないマルウェアの場合でも、マルウェアによる機密情報へのアクセスをブロックします。
- 可能な限り早期に、マルウェアを識別し駆除します。マルウェアを駆除することで、ブロックすることが難しい、またはブロックするセキュリティソリューションを攻撃する亜種にマルウェアが変化しないよう阻止できます。さらに、Trusteer Rapportでは、マルウェアの亜種がどのようなバイナリファイルを使用している場合でも、同じマルウェアから派生した複数の亜種を検知し、駆除できます。
- 識別されているマルウェアを、知らないうちにダウンロードしてしまうことを防止します。これは正規のWebサイトからダウンロードする場合も同様です。

危機にさらされているもの

悪意のあるソフトウェアは、正規のWebサイトから、知らないうちにコンピューターにダウンロードされてしまうことがよくあります。悪意のあるソフトウェアおよびPCについては、以下のような憂慮すべき事実が判明しています。

- 200万の正規のWebサイトが、ユーザーの知らないうちに、ユーザーのPCにマルウェアをダウンロードしています(Sophos社、2008年4月)。
- 毎日15,000のWebページで、新たにウィルスに感染していることが特定されています。このうち79%は、ハッキングされた正規Webサイトです。GoogleやYahooなどの広く認知されているWebサイトでも、広告を介してユーザーにマルウェアを提供してしまっていることが報告されています。非常に慎重で、広く認知されているWebサイトしか閲覧しないユーザーの場合でも、マルウェアはコンピューターに侵入する機会を見つめます(Sophos社、2008年4月)。
- 業界トップクラスのアンチウィルスベンダーによるテストおよびWebブラウザのアンチフィッシングフィルターによると、インターネット上では過半数のアクティブなマルウェアおよびフィッシングの脅威が検知されておらず、平均検知率はマルウェアでは37%、フィッシングでは42%にとどまっています(Cyveillance社、2009年2月)。
- 米国においてはパーソナルコンピューターの4分の1 (つまり5,900万台) は、すでにマルウェアに感染しています(経済協力開発機構(OECD)、2008年6月)。
- 最近のマルウェアは、ユーザーに気付かせずにキーストロークを記録し、スクリーンイメージをキャプチャーして、コンピューターから金融情報を盗むことができます。

Trusteer Rapportが必要とされる理由

Trusteer Rapportの保護は、従来のデスクトップセキュリティソリューションで使用されているテクノロジーとは全く異なる、革新的なテクノロジーに基づいています。Trusteer Rapportは、スタンドアロンで使用することも、デスクトップセキュリティソリューションと併用することも可能です。このアプリケーションはアンチウィルスの代わりになるものではなく、アンチウィルスソリューションではありません。ご使用のコンピューターで最新のアンチウィルスソリューションを実行している場合でも、Trusteer Rapportを使用する必要があります。

アンチウィルス、ファイアウォール、およびその他のセキュリティソフトウェアは重要ですが、残念ながら十分な効果があるとは言えません。さまざまな研究および最近のインシデントでは、これらのツールは銀行口座からお金を盗み出す犯罪を防ぐには、必ずしも十分でないことが分かっています。犯罪の高度化に伴い、銀行では安全なオンラインバンキングを実現するため、ユーザーのコンピューターで追加の保護レイヤーを利用することを推奨しています。

アンチウィルスソフトウェア、アンチスパイウェアソフトウェア、個人のファイアウォールおよびアンチフィッシングツールバーなどの従来のソリューションは、既知の不正な動作のリスト(シグネチャ、ヒューリスティック、ブラックリストなど)に依存しています。これらのソリューションは、最新の、非常に高度な金融詐欺およびなりすまし犯罪の手法には、効果がなくなりつつあります。これらの攻撃は非常に危険であり、深刻な金融上の損害を被るおそれがあります。

「業界トップクラスのアンチウィルスベンダーによるテストおよびWebブラウザのアンチフィッシングフィルターによると、インターネット上では過半数のアクティブなマルウェアおよびフィッシングの脅威が検知されておらず、平均検知率はマルウェアでは37%、フィッシングでは42%にとどまっています。」
(Cyveillance社、2009年2月)

最近のマルウェアは、オンラインバンキング、証券取引、ショッピング、eコマース、電子メール、およびソーシャルネットワーキングWebサイトからログイン認証情報を盗むことができます。Webサイトでセキュリティが確保されている場合でも、犯罪者はお客様のオンライン口座を使用して、不正なトランザクションの実行、発注、電子メールの送信、およびその他の操作を実行できます。

Trusteer Rapportは、ユーザー名、パスワード、またはその他の機密ログイン情報が安全でないWebサイトに送信されないように保護することで、マルウェアおよび不正なWebサイトによる機密情報の窃盗や、Web通信のハイジャックを防止します。また、Trusteer Rapportはオンライン通信を保護し、マルウェアによりユーザーのトランザクションが改ざんされないようにします。たとえば、Trusteer Rapportは、ユーザーの銀行口座から犯罪者の銀行口座に送金するソフトウェアからユーザーを保護します。オンラインバンキング、トレード、ショッピングを利用する場合、Trusteer Rapportを使用していれば、ますます増加する金融詐欺およびなりすまし犯罪にさらされる危険性を大幅に低減できます。

Trusteer Rapportとインターネットセキュリティスイートとの違い

Trusteer Rapportは、インターネットセキュリティスイートとは全く異なります。インターネットセキュリティスイートは、悪意のあるソフトウェアおよび悪質なWebサイトのデータベースで構成されており、これを使用してコンピューター上で脅威を検知し、駆除します。インターネットセキュリティスイートのベンダーは、データベースを更新するために、常に新しい悪意のあるソフトウェアおよび悪質なWebサイトを探しています。Trusteer Rapportは、これとは全く異なるテクノロジーを使用しています。

Trusteer Rapportは、ユーザーが銀行のWebサイトにアクセスしたとき、これを認識します。また、トランザクションの実行時、ログイン情報の送信時、および機密の銀行口座明細の読み取り時にも、これを認識します。その際、Trusteer Rapportはアクセスコントロールレイヤーをユーザーの機密情報に適用して、悪意のあるソフトウェアおよび悪質なWebサイトが、ユーザーの機密情報やトランザクションにアクセスしたり、改ざんしたりしないように防止します。パスワードの読み取りや、トランザクションの変更の試行などの、不正アクセスの試行はただちにブロックされます。Trusteer Rapportのアクセスコントロールポリシーは、銀行により設定されています。

Trusteerと連携している銀行は、どの機密情報が制限されるか、およびその機密情報に対するどのような操作が制限されるかを定義するポリシーを作成し、保持します。インターネットセキュリティスイートとは異なり、Trusteer Rapportは悪意のあるソフトウェアおよびWebサイトのデータベースは保持しないため、インターネットセキュリティスイートではまだ認識されていない新しい脅威や、「気付かれていない」脅威をブロックすることができます。銀行とTrusteerは、現在オンライン銀行をターゲットにしている金融犯罪に対して、Trusteer Rapportは効果的であり続けるように、懸命に努力しています。

Trusteer Rapportで保護できる攻撃

Trusteer Rapport独自のブラウザーロックダウンテクノロジーにより、顧客とWebサイト間でやりとりされる機密情報に対する不正アクセスは、その脅威を引き起こしている特定のマルウェアがどのようなものであっても、ブロックされます。

Trusteer Rapportは、以下のすべての手法をブロックするうえで効果的です。

- [フィッシング\(11ページ\)](#)
- [ファームिंगまたはDNS偽装\(12ページ\)](#)
- [キーロギング\(12ページ\)](#)

- [中間者攻撃\(13ページ\)](#)
- [マンインザブラウザ攻撃\(13ページ\)](#)
- [スクリーンキャプチャー\(14ページ\)](#)
- [セッションハイジャック\(14ページ\)](#)
- [自動ダウンロード\(15ページ\)](#)

フィッシング

フィッシング攻撃では、犯罪者はユーザーが知っており、信頼しているWebサイト(たとえば、ご使用の銀行のWebサイトなど)にそっくりのWebサイトを構築します。その後、犯罪者はユーザーにそのWebサイトを閲覧するように促します(たとえば、そのWebサイトへのリンクが含まれた偽の電子メールを送るなど)。ユーザーがその不正Webサイトにアクセスすると、ユーザーはそれが正規のWebサイトであると誤信します。ユーザーがその不正Webサイトでサインインを試行すると、犯罪者はただちにユーザーのサインイン認証情報を入手します。その後、犯罪者はその認証情報を使用して、ユーザーになりすまして正規のWebサイトにサインインします。

ユーザーをフィッシング攻撃から保護するため、Trusteer Rapportは以下のように対応します。

- 悪意のあるWebサイトであることが分かっているWebサイトにアクセスした場合、ユーザーに警告します。
- データを安全に送信しないWebサイトにユーザーがパスワードを入力した場合、ユーザーに警告します。データを安全に送信しないサイトはリスクの高いサイトであり、犯罪者が簡単に情報をインターセプトできる正規Webサイトも含まれます。

ファージングまたはDNS偽装

ファージングまたはDNS偽装攻撃では、ユーザーがブラウザのアドレスバーに正規のWebサイトのアドレスを入力するたびに、不正なWebサイトに接続するように、犯罪者がコンピューターを操作します。この攻撃は、デスクトップにマルウェアを感染させたり、ご使用のISPのネットワーク内サーバーを攻撃したりするなどの、さまざまな方法で行われます。ユーザーが不正なWebサイトにアクセスし、サインインを試行してしまうと、犯罪者はユーザーのサインイン認証情報を入手します。その後、犯罪者はその認証情報を使用して正規のWebサイトにサインインし、ユーザーになりすまして不正なトランザクションを実行します。ユーザーをファージング攻撃から保護するため、Trusteer Rapportは、ユーザーが保護されたWebサイトに接続するたびに、そのWebサイトのIPアドレスおよびSSL証明書を検証します。この検証が失敗すると、その接続はTrusteer Rapportにより切断され、正規のWebサイトへの接続が確立されません。

キーロギング

キーロガーは、ユーザーが気付かないままコンピューター内に存在している悪意のあるプログラムです。キーロガーは、ユーザーがキーボードを使用して文字を入力したときに、キーストロークを記録して、その情報を犯罪者に送信します。この方法では、ユーザーの入力操作から、キーロガーがログイン認証情報やクレジットカード番号、およびその他の機密情報を入手し、その情報を犯罪者に送信します。犯罪者は、その認証情報を使用して銀行口座にログインし、ユーザーになりすまして不正なトランザクションを開始します。Trusteer Rapportは、キーロガーが機密情報を読み取ることができないようにキーストロークを暗号化することで、キーロガーをブロックします。

中間者攻撃

中間者攻撃は、フィッシングおよびファームウェア攻撃が進化したものです。この攻撃では、ユーザーがWebサイトにサインインして操作を行ったときに、ユーザーが全く気付かないうちに、ユーザーとそのWebサイト間でやりとりされたすべての情報が、中間Webサイトを介して犯罪者に送信されます。この中間Webサイトでは、あらゆる個人情報が閲覧され、ユーザーが行ったトランザクションが改ざんされます。たとえば、ユーザーが特定の金額を受取人に対して送金することを要求した場合、犯罪者はその受取人のIDを変更して、その金額が別の口座に振り込まれるようにすることができます。

Trusteer Rapportは、WebサイトIPアドレスやWebサイトの証明書が正規のものであることを検証するなど、複数の検証レイヤーを使用して、ブラウザーにより不正なサイトへの悪質なリダイレクトを防止します。

マンインザブラウザー攻撃

マンインザブラウザー攻撃は、ユーザーのブラウザーに侵入するマルウェアです。これは、ツールバー、BHO、ブラウザーのプラグインなどの正規アドオンの形で侵入する場合があります。このマルウェア感染すると、ブラウザー内で発生するすべての動作が制御されてしまいます。このマルウェアは、ユーザーのサインイン認証情報などの機密情報を読み取り、犯罪者に送信することができます。また、ユーザーになりすまして、ユーザーの口座から犯罪者の口座に送金するなどの、トランザクションを作成することも可能です。

Trusteer Rapportは、以下の複数のメカニズムにより、マルウェアがブラウザー内のデータに接触することを防ぎます。

- まだ認識されていないマルウェアの場合でも、マルウェアによる機密情報へのアクセスをブロックします。

- 可能な限り早期に、マルウェアを識別し駆除します。マルウェアを駆除することで、ブロックすることが難しい、またはブロックするセキュリティソリューションを攻撃する亜種にマルウェアが変化しないよう阻止できます。さらに、Trusteer Rapportでは、マルウェアの亜種がどのようなバイナリファイルを使用している場合でも、同じマルウェアから派生した複数の亜種を検知し、駆除できます。
- 識別されているマルウェアを、知らないうちにダウンロードしてしまうことを防止します。これは正規のWebサイトからダウンロードする場合も同様です。

スクリーンキャプチャー

マルウェアには、画面をキャプチャーして犯罪者に送信する、スクリーンキャプチャーメカニズムが含まれている場合があります。スクリーンショットには、口座の詳細情報、残高、さらにWebサイトのログインページにキーパッドが使用されている場合は、認証情報までも含まれる場合があります。Trusteer Rapportは、保護されたWebサイトに接続している間、スクリーンキャプチャーメカニズムを無効にします。

セッションハイジャック

セッションハイジャックマルウェアは、特定Webサイトとのセッションで使用されたパラメーターを盗み、その情報を犯罪者に送信します。その後、犯罪者はこのセッションパラメーターを使用してWebサイトとのセッションを乗っ取り、Webサイトにログインする際に要求される認証を回避します。Trusteer Rapportは、保護されたWebサイトに接続している間、セッションパラメーターへのアクセスを防止します。

自動ダウンロード

自動ダウンロードでは、Webサイトにアクセスするだけで、ユーザーが気付かないうちに悪意のあるマルウェアがダウンロードされます。そのようなWebサイトは、ウィルスに感染した正規のWebサイトである場合もあるため、ユーザーが知らないうちにマルウェアがコンピューターにダウンロードされてしまうのです。

Trusteer Rapportの動作原理

Trusteer Rapportをコンピューターにインストールすると、Trusteerと連携しているパートナー企業に属するWebサイトが自動的に保護され、その企業および顧客に対して最高レベルのセキュリティが提供されます。また、Trusteer Rapportを使用すると、ユーザーは手動でRapportの保護を使用しているその他のすべてのWebサイト(サインインして個人の金融情報や機密データなどの機密情報をやりとりするWebサイト)に適用できます。

保護されたWebサイトに接続すると、Trusteer Rapportはバックグラウンドで以下の3つの主要な動作を実行します。これにより、ユーザーが犯罪者のターゲットになることが、きわめて困難になります。

- Trusteer Rapportは、犯罪者が作成した偽のWebサイトではない、正規のWebサイトに接続しているかどうかを検証します。驚くべきことに、WebブラウザーにWebサイトのアドレスを入力しても、必ずしも正規のWebサイトに接続するとは限りません。
- 検証が完了すると、Trusteer Rapportは、ユーザーのコンピューターと保護されたWebサイト間の通信をロックダウンします。これにより、犯罪者は、ユーザーと銀行とのオンライン接続をハイジャックできなくなります。

- Trusteer Rapportは、銀行または企業と安全に接続するための通信トンネルを作成し、犯罪者がマルウェアを使用してログインデータを盗んだり、金融トランザクションややりとりする情報を改ざんしたりできないようにすることで、ユーザーのコンピューターおよびインターネット接続を保護します。

Trusteer Rapportは、非常に重要で、他には無いセキュリティレイヤーを追加します。これを利用することで、パートナーはより適切にユーザーの機密情報を保護し、直接ユーザーをターゲットにした脅威に素早く対応できるようになります。

以下に、Trusteer Rapportがユーザーの通信、データ、および金融資産を保護する具体的な方法の一部を示します。

- [保護されたサイトとの安全な通信\(17ページ\)](#)
- [ログイン保護\(17ページ\)](#)
- [ブラウジングセッション保護\(18ページ\)](#)
- [キーストローク保護\(18ページ\)](#)
- [クレジットカード保護\(19ページ\)](#)
- [スクリーンキャプチャーのブロック\(19ページ\)](#)
- [Webサイト検証\(19ページ\)](#)
- [ブラウザーアドオンのブロック\(20ページ\)](#)
- [プロセス変更のブロック\(20ページ\)](#)
- [悪意のあるWebサイトの警告\(20ページ\)](#)
- [不正アクセスのレポート\(21ページ\)](#)

保護されたサイトとの安全な通信

ユーザーが保護されたWebサイトに接続すると、Trusteer Rapportにより、コンピューター上で行われるあらゆるプロセスからの、そのWebサイトへのアクセスがブロックされます。ユーザーは、マルウェアによる悪意のあるアクセス試行からシールドされた状態で、Webサイトと安全に通信することができます。ユーザーのコンピューターに、認識されていないマルウェアが潜んでいる場合でも、そのマルウェアによりWebサイトから機密情報が読み取られたり、ランザクションが改ざんされたりすることはありません。

ログイン保護

ユーザーが保護されたWebサイトにサインインすると、Webサイトはセキュアなログイン認証情報(ユーザー名とパスワードなど)を使用してユーザーを認証します。問題は、犯罪者は複数の方法を使用してユーザーのログイン認証情報を入手し、その情報を使用してユーザーのオンライン口座にサインインすることです。

その方法の1つは、フィッシングと呼ばれています。フィッシング攻撃では、ユーザーは正規のWebサイトに見せかけた偽のWebサイトに誘導され、不正なWebサイトであることに気が付かないまま、そのWebサイトに認証情報を入力してしまいます。こうしてログイン認証情報を入手した犯罪者は、その認証情報を使用してユーザーになりすまし、ユーザーのオンライン口座にサインインできます。

Trusteer Rapportは、ユーザーが悪意のあるWebサイトであることが判明しているWebサイトにアクセスしようとしたり、データを安全に送信しないWebサイトに誤ってログイン情報を入力してしまったりしたときに、警告を表示することでユーザーをフィッシング攻撃から保護します。

ブラウジングセッション保護

Webサイトにログインすると、そのWebサイトではセッションの間、セッションクッキーと呼ばれるテキストファイルが一時メモリーに保存されます。セッションクッキーはユーザーの認証済みセッションを識別し、その都度ログインし直さなくても、そのWebサイトのサーバーとの間で繰り返し機密情報をやり取りできます。

マルウェアはセッションクッキーを入手し、それを利用して認証を回避することで、ユーザーとWebサイト間のセッションを乗っ取ります。この種の攻撃からユーザーを保護するために、Trusteer Rapportは、パートナーのWebサイト上にあるセッションクッキーにアプリケーションがアクセスしないようにブロックします。

注: この機能は、Trusteerと連携して顧客のオンライン通信を保護しているパートナーの場合のみサポートされています。

キーストローク保護

Trusteer Rapportは、ブラウザーに送られるキーストロークを暗号化し、キーロガーと呼ばれる悪意のあるプログラムや、オペレーティングシステムに潜んでいる悪意のあるソフトウェアコンポーネントから、キーストロークを隠します。これにより、マルウェアがキーストロークを読み取って、パスワードやクレジットカード番号などの機密情報を入手することを防止します。

クレジットカード保護

Trusteer Rapportは、ユーザーがクレジットカード情報をローカルの安全でないWebサイトに送信すると、警告を表示します。この警告が表示されるダイアログボックスを使用して、送信を止めることができます。また、Rapportは、Rapportにより保護されたサイトまたはVisa、MasterCard、Amexなどのクレジットカードに関連するキーワードが含まれるその他の安全な(https)サイトにユーザーがクレジットカード番号を入力すると、アンチキーロギング機能をアクティブにします。アンチキーロギング保護は、キーロギングマルウェアによりクレジットカードの詳細がキャプチャーされないようにします。

注: この機能は、登録しているカード会社によって発行されたカードのみでサポートされています。

スクリーンキャプチャーのブロック

Trusteer Rapportは、保護されたWebサイトがブラウザーに表示されている間、あらゆるスクリーンキャプチャーの試行を無効にします。これにより、マルウェアが画面をキャプチャーすることで、機密情報を入手してしまうことを防止します。

Webサイト検証

銀行または企業Webサイトの正しいアドレスを入力したとしても、悪意のあるソフトウェアは、(ファーミング攻撃と呼ばれる)複数の方法を使用して、ブラウザーを不正なWebサイトにリダイレクトします。

ユーザーをファージング攻撃から保護するため、Trusteer Rapportは、ユーザーが保護されたWebサイトに接続するたびに、そのWebサイトのIPアドレスおよびSSL証明書を検証します。SSL証明書が古い、間違っている、または不明な発行者によって署名されている場合は、Rapportは警告を表示し、ユーザーがそのサイトに接続することを回避できるようにします。対象Webサイトの信頼済みIPアドレステーブルで、対象のIPアドレスが見つからない場合、Rapportにより、そのIPアドレスは対象Webサイトの既知の問題ないIPアドレスに変更されます。

ブラウザーアドオンのブロック

保護されたWebサイトに接続すると、Trusteer Rapportにより、正規の安全なソフトウェアであると認識されていないブラウザーアドオンは、すべてブロックされます。ブラウザーアドオンは、ブラウザー内に組み込まれる小さな(通常はサードパーティー製)ソフトウェアで、ブラウザーの通信をコントロールするものです。この機能は、ログイン情報を盗んだり、通信を改ざんしたりするおそれのある悪意のあるブラウザーアドオンから、ユーザーを保護します。

プロセス変更のブロック

Trusteer Rapportは、ブラウザープロセスを変更しようとする試みを解析し、疑わしいものはブロックします。ブラウザープロセスの変更(ファンクションパッチとも呼ばれる)は、ブラウザーを乗っ取り、機密情報へのアクセスを可能にする手法です。

悪意のあるWebサイトの警告

Trusteer Rapportは、ユーザーが悪意のあるWebサイトであることが分かっているWebサイトにアクセスした場合、ユーザーに警告します。

不正アクセスのレポート

Trusteer Rapportは、TrusteerのパートナーWebサイトと通信して、セキュリティレベルについてのフィードバックを提供したり、オンライン口座にアクセスしようとしたあらゆる不正試行をレポートしたりします。これにより銀行または企業は脅威に迅速に対応することができます。

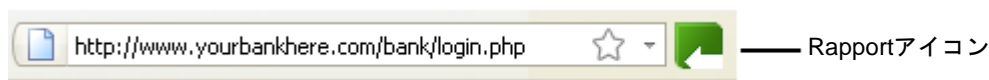
注: この機能は、Trusteerと連携して顧客のオンライン通信を保護しているパートナーの場合のみサポートされています。


ユーザーエクスペリエンス

Trusteer Rapportは、非常に使いやすいアプリケーションです。Trusteer Rapportを使用するために、技術的な知識は必要ありません。Trusteer Rapportは設定を必要とせず、ユーザーの操作内容やブラウザの動作を変更することもなく、またセキュリティの脅威に遭遇したときに、ユーザーに技術的な質問をすることもありません。

Trusteer Rapportの保護アクティビティのほとんどは、ユーザーに気づかれずに実行されるため、ユーザーの操作の邪魔になったり、ユーザーの介入が必要になったりすることはありません。Rapportは、[「Trusteer Rapportのアクティビティの表示」](#) (166ページ)で説明されているように、ユーザーを保護するために実行したすべてのアクションを、ユーザーが随時閲覧できる形で記録しています。リスクレベルに関する詳細は、アクティビティレポートに記載されています。Rapportがリスクの高い脅威に遭遇すると、Rapportはユーザーに通知します。このような場合、一部の保護アクションでは、[「アラートおよび警告への応答」](#) (92ページ)で説明されているように、簡単な応答が必要な場合があります。

どのWebサイトがTrusteer Rapportによって保護されているかは、簡単に確認できます。ご使用のブラウザのアドレスバー上または右端に表示されているアイコンの色により、現在表示されているサイトが保護されているかどうか分かります。



Rapportのアイコン()は、Trusteer Rapportが実行されているときに、Windowsのシステムトレイに表示されます。トレイアイコンをクリックすると、Trusteer Rapportのコンソールが開きます。このコンソールから、さまざまなTrusteer Rapportの機能および情報にアクセスできます。

保護されたサイトで新しいログイン情報を使用すると、Trusteer Rapportのダイアログボックスが表示され、[「パスワード保護の提示に対する応答」](#) (107ページ)で説明されているように、パスワード保護が提示されます。このダイアログボックスは、そのログイン情報を初めて入力した場合のみ、表示されます。

Trusteer Rapportの有効活用

TrusteerパートナーのWebサイトに接続したときに、保護が自動的に提供されるほか、ユーザーは、使用しているその他すべての機密性の高いWebサイトに対して、手動でTrusteer Rapportの保護を追加できます。「追加のWebサイト保護」および「Login Details」を参照してください。

Trusteer Rapportは、Webサイト保護の以外にも、以下のようなセキュリティ機能も提供しています。これらはすべて無償で含まれています。

- コンピューターのセキュリティを向上します([「セキュリティ向上のためのコンピューターのスキャン」](#) (170ページ)を参照)。
- オンラインの銀行口座に侵入しようとした試みについてのレポートを生成します([「Trusteer Rapportのアクティビティの表示」](#) (166ページ)を参照)。

- Trusteerから、Rapportコンソールの専用スパムフリーインボックスに直接配信されるセキュリティに関するニュースを受信できます([「セキュリティニュースの受信」](#) (175ページ)を参照)。

高度なユーザーのための情報

Trusteer Rapportは、負担の少ないソフトウェアアプリケーションです。Rapportのフットプリントの詳細については、[「Trusteer RapportのPCフットプリント」](#) (23ページ)を参照してください。

Trusteer Rapportは、いかなる形でも、ユーザーのプライバシーを侵害することはありません。[「Trusteer Rapportとお客様のプライバシー」](#) (24ページ)を参照してください。

Trusteer Rapportには、マルウェアによるソフトウェアの停止または削除を防ぐための、自己保護メカニズムが組み込まれています。そのため、タスクマネージャーを使用して、プロセスを終了することはできません。Trusteer Rapportの停止の詳細については、[「Trusteer Rapportの停止」](#) (207ページ)を参照してください。

Trusteer RapportのPCフットプリント

Trusteer Rapportのフットプリントには、以下の内容が含まれます。

- 実行可能ファイル:
 - Program Files¥Trusteer¥Rapport¥bin¥RapportService.exe、
 - Program Files¥Trusteer¥Rapport¥bin¥RapportMgmtService.exe
- プロセス: RapportService.exe、RapportMgmtService.exe
- サービス: Rapport管理サービス(64ビットオペレーティングシステムの管理者アカウント以外: RapportInjService_x64.exe)
- ドライバー:

- RapportPG.sys (64ビットオペレーティングシステムの場合:
RapportPG64.sys)
- RapportKELL.sys (64ビットオペレーティングシステムの場合:
RapportKE64.sys)
- RapportEI.sys (64ビットオペレーティングシステムの場合:
RapportEI64.sys)
- ログおよび設定用として、平均15MB程度のユーザープロファイル用領域を想定(マシンで使用されている異なるブラウザの数に応じて異なり、これ以上の大きさになる場合もある)
- プログラムのサイズは、15MB + ユーザープロファイル用領域

Trusteer Rapportとお客様のプライバシー

Trusteer Rapportは、ご使用のコンピューター上で、ユーザーの認証情報の暗号化されたシグネチャを作成します。この情報を使用してユーザーの認証情報を取得することはできません。Trusteer Rapportは、この情報を使用して、ユーザーの認証情報が不正に漏洩していないかを特定します。Trusteer Rapportは、`sekyuri`および内部エラーに関する匿名のレポートを、[「Trusteer Rapportセントラルサービス: 強力な詐欺行為ブロック機能」](#) (24ページ)に送信します。この情報は、製品およびポリシーを改善するために使用されます。

Trusteer Rapportセントラルサービス: 強力な詐欺行為ブロック機能

Trusteer Rapportセントラルサービスは、Trusteer Rapportがパートナーに提供しているサービスであり、パートナーはこのサービスを利用して、ユーザーの口座で不正なアクティビティが行われないように、ただちにアクションを実行することができます。

Trusteer Rapportが疑わしいソフトウェアまたはWebサイトアクティビティを検知すると、その都度セキュリティイベントが生成され、Trusteer Rapportセントラルサービスに送信されて解析されます。セントラルサービスは、徹底したテストを実行して、そのアクティビティが不正であるかどうか特定されません。不正なアクティビティであった場合は、セントラルサービスからTrusteer Rapportに対して、より積極的にその脅威をブロックするように指示されます。

注: Trusteer Rapportセントラルサービスは、ユーザーが解析のためのセキュリティイベントの送信を無効にしていない場合のみ、ご使用の銀行が利用できるサービスです。この設定はTrusteer Rapportの設定ウィザードに含まれており、デフォルトでは有効になっています。この設定を有効にした場合、完全な匿名性¹が保証されます。

Trusteer Rapportは、セキュリティイベントを送信して解析を受けることを選択しなくても、保護を提供します。ただし、解析用にイベントを送信することで、Rapportはより高度な未知の脅威も検知できるようになります。

以下に、Trusteer Rapportが解析用に送信するセキュリティイベントの例をいくつか示します。

- 疑わしいWebサイト
- 認証情報のキャプチャーが試行された場合
- 機密性の高い通信への干渉が試行された場合
- 疑わしいソフトウェア

Trusteer Rapportセントラルサービスの最大のメリットの1つは、ユーザーのユーザー名およびパスワードが危険にさらされた場合、銀行に対して警告を通知する早期警告システムです。セントラルサービスは、アンチウィルスやその他のセキュリティソフトウェアをかいくぐった脅威を検知することができます。

¹ ご使用のコンピューターからTrusteer Rapportセントラルサービスに送信されるすべての情報は匿名であり、技術的な詳細情報が含まれるだけで、個人情報を含みません。ユーザーの個人情報が危険にさらされている可能性が疑われる場合、Trusteer Rapportは、銀行または企業に対して警告を送信します。この警告にはIDが含まれており、銀行または企業はこのIDを使用してインシデントとユーザーの口座に関連付けることができます。Trusteerは、このIDや、その他の個人情報を知ることはできません。

セキュリティイベントの他にも、Trusteer Rapportはソフトウェアの内部エラーについての情報も随時送信します。この情報は、Trusteerがソフトウェアの問題を特定し、修復するために役立ちます。

セキュリティイベントおよびエラーログのTrusteerへの送信の無効化についてTrusteerへのセキュリティイベントおよびエラーログの送信が有効になっている場合、完全な匿名性²が保証されます。弊社ではお奨めしませんが、ご希望に応じてこの機能を無効にすることができます。

セキュリティイベントおよびエラーログのTrusteerへの送信を無効にするには、[「セキュリティコントロールの変更」](#) (189ページ)の説明に従って、[セキュリティイベントおよびエラーを分析のために送信する]を[常に]から[しない]に変更してください。

² ご使用のコンピューターからTrusteer Rapportセントラルサービスに送信されるすべての情報は匿名であり、技術的な詳細情報が含まれるだけで、個人情報に含まれません。ユーザーの個人情報が危険にさらされている可能性が疑われる場合、Trusteer Rapportは、銀行または企業に対して警告を送信します。この警告にはIDが含まれており、銀行または企業はこのIDを使用してインシデントとユーザーの口座に関連付けることができます。Trusteerは、このIDや、その他の個人情報を知ることはできません。

3. Trusteer Rapport のインストール

Trusteer Rapportは、素早く簡単にインストールできます。銀行または企業のWebサイトからインストールファイルをダウンロードし、ファイルを実行して、標準インストールウィザードの指示に従うだけでインストールできます。

Trusteer Rapportのダウンロードおよびインストールについての詳細説明が必要な場合は、本項の関連トピックを参照してください。

注: Windows管理者アカウントからTrusteer Rapportをインストールすると、標準ユーザーはTrusteer Rapportを自分のアカウントから実行できますが、Trusteer Rapportの停止、開始、アンインストール、オーバーインストール、および特定のポリシー設定の変更はできません。これは、管理者がTrusteer Rapportを企業全体にインストールし、個々の従業員がセキュリティ機能を無効にしたり、すべてのユーザーのセキュリティポリシーを変更したりしないように制限するために設けられている機能です。

管理者アカウントからTrusteer Rapportをインストールすると、Trusteer Rapportの保護が自動的にすべてのユーザーに拡張されます。また、Trusteer Rapportの最も重要な保護メカニズム(マルウェアの防止と駆除)はドライバーからインストールされますが、標準ユーザーアカウントからインストールすると、ドライバーがインストールされません。そのため、Trusteer Rapportは管理者アカウントからインストールすることを強くお勧めします。

Trusteer Rapportを標準ユーザーアカウントからインストールすると、Trusteer Rapportはその他のユーザーアカウントでは実行されず、いったんアンインストールしないと、その他のいかなるアカウントにもインストールできません。

管理者アカウントへの切り替え方法

- [「管理者アカウントへの切り替え\(Windows 7\)」](#) (152ページ)
- [「管理者アカウントへの切り替え\(XP\)」](#) (154ページ)
- [「管理者アカウントへの切り替え\(Vista\)」](#) (156ページ)

Trusteer Rapportのダウンロード場所

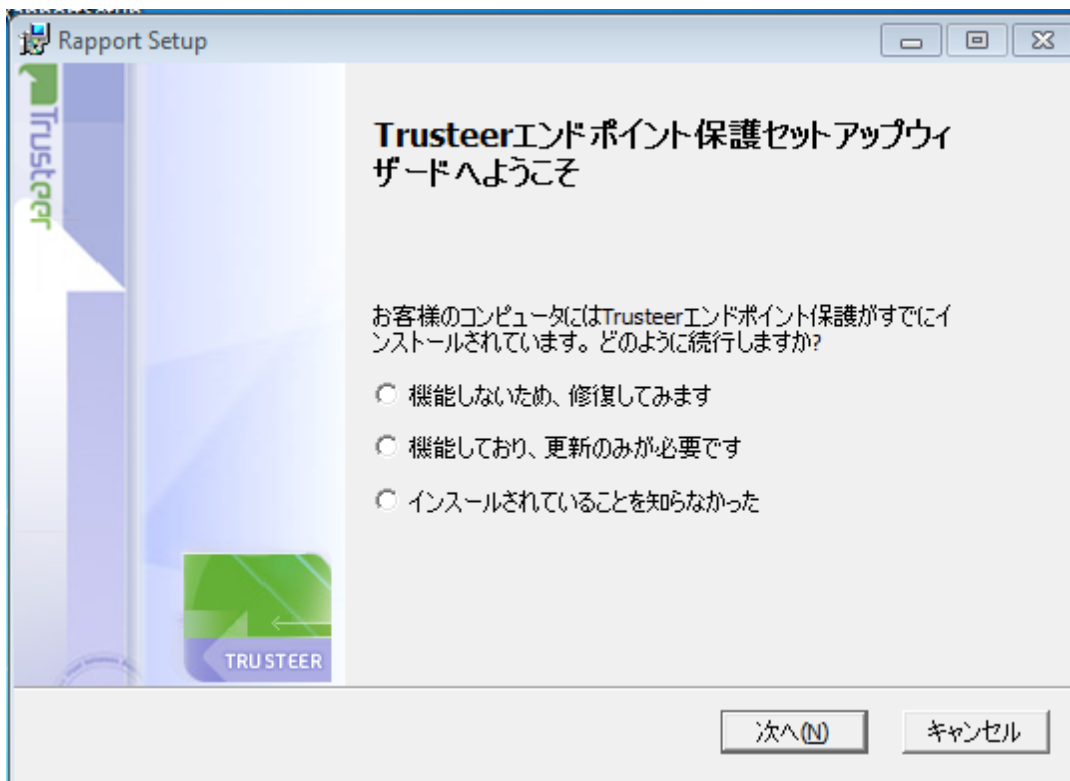
Trusteer Rapportを提供している銀行またはその他の組織の顧客の方は、銀行のWebサイトからRapportをダウンロードできます。銀行からは、以下のような方法で提供されます。

- 銀行のWebサイト上(通常はページの下部)にセキュリティセクションを表示し、そこにTrusteer Rapportへのリンクまたは「ユーザー様ご自身の保護」のリンクを表示します。
- オンライン口座へのログインプロセスの一部として、または正常にログインした直後に、Trusteer Rapportのダウンロードを促します。

Trusteer Rapportの対応オペレーティングシステムおよびブラウザについて Trusteer Rapportの対応オペレーティングシステムおよびブラウザについては、以下を参照してください。 <http://www.trusteer.com/supported-platforms>

使用しているコンピューターにTrusteer Rapportがすでに存在していると表示される場合

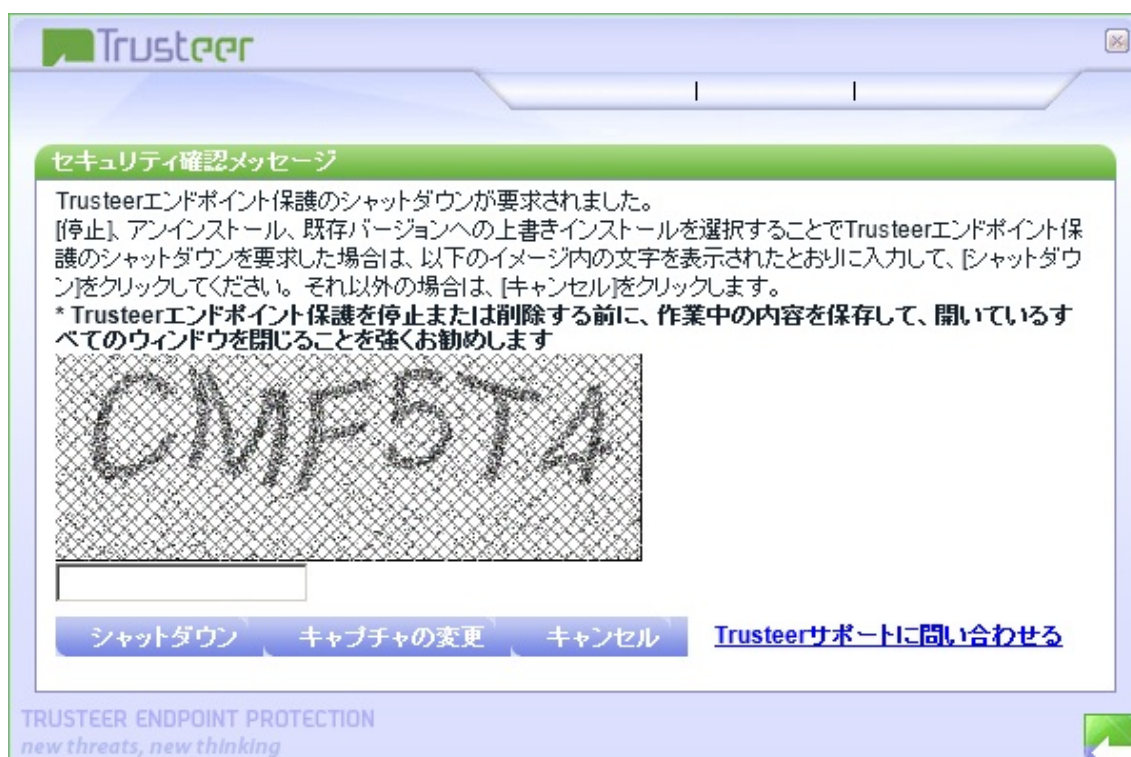
Trusteer Rapportをインストールする際、ご使用のコンピューターに任意のバージョンのTrusteer Rapportがすでに存在している場合、インストールプロセス中に、以下のダイアログボックスが表示されます。



インストール中にこの画面が表示された場合、ご使用のコンピューターにはすでにTrusteer Rapportがインストールされていることを意味します。Rapportを再インストールしても、安全性は全く問題ありません(ただし新しいバージョンを古いバージョンで上書きしてしまった場合を除く)。

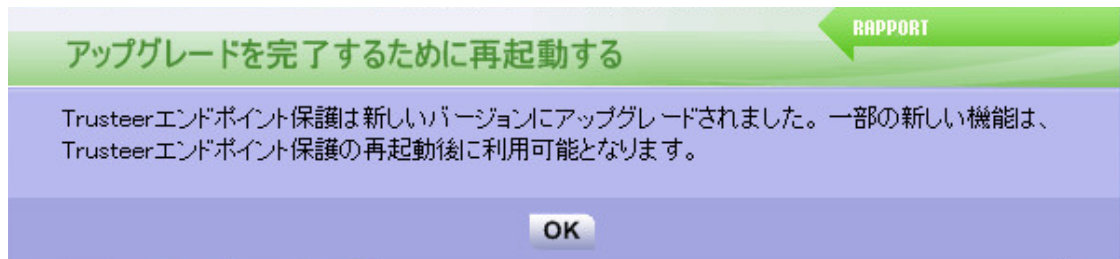
➔ 既存バージョンの上書きによるTrusteer Rapportのインストール方法

1. Trusteer Rapportを再インストールする理由を最もよく表しているオプションを選択します。
2. [次へ]をクリックします。インストールプロセスが開始された後、Trusteer Rapportをシャットダウンするためにいったんプロセスが中断されます。Rapportがシャットダウンする前に、セキュリティ確認メッセージが表示されます。このメッセージでは、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアによりRapportが無効化されることを防止するためのものです。



3. 画像に表示された文字を入力します(大文字、小文字は識別されません)。

4. [シャットダウン]をクリックします。Rapportのシャットダウン中に、[Rapportがシャットダウンするまでお待ちください...]というメッセージが表示されます。Rapportが動作を停止すると、メッセージが消えます。その後、インストールプロセスが通常どおりに続行されます。インストール後、以下の画面が表示される場合があります。



このメッセージが表示された後も、ご使用のコンピューターは安全です。ただし、できるだけ早くコンピューターを再起動することをお奨めします。

共有仮想デスクトップ環境でのTrusteer Rapportのインストール方法

Trusteer RapportをWindows Server (2003または2008)にインストールする場合、インストールウィザードによりOSが検知され、Trusteer Rapportのサーバーバージョンがインストールされます。このバージョンでは、複数のセッションがサポートされます。詳細については、[「Windows Server \(2003または2008\)へのTrusteer Rapportのインストール」](#) (67ページ)を参照してください。

Internet Explorer を使用した Windows 7 への Trusteer Rapport のインストール

この手順では、Windows 7 を実行しており、ブラウザは Microsoft Internet Explorer を使用している場合の Trusteer Rapport のダウンロードおよびインストール方法を説明します。

➔ Trusteer Rapport のインストール方法

1. 組織のログインページをブラウズします。組織から Trusteer Rapport のダウンロードが提供されている場合は、**[ダウンロード]** ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。

御行のロゴはこちらへ

オンラインバンキング利用時に必須のセキュリティー

Trusteer Rapport をダウンロード

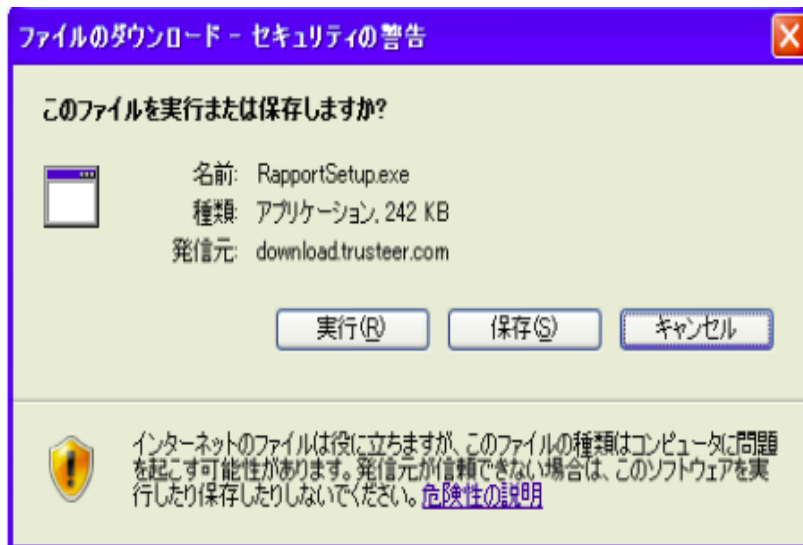
-  お客様の個人情報や銀行口座情報を、認証情報の盗難や詐欺から守ります。
-  各アンチウイルスソフトウェアと共存しながらも、それらのソフトウェアでは阻止できない攻撃からお客様を守ります。
-  効果的にお客様の環境を守る Trusteer Rapport は、簡単な使用方法で、お客様のコンピューターの減速を招くことはありません。

[今すぐダウンロード](#)

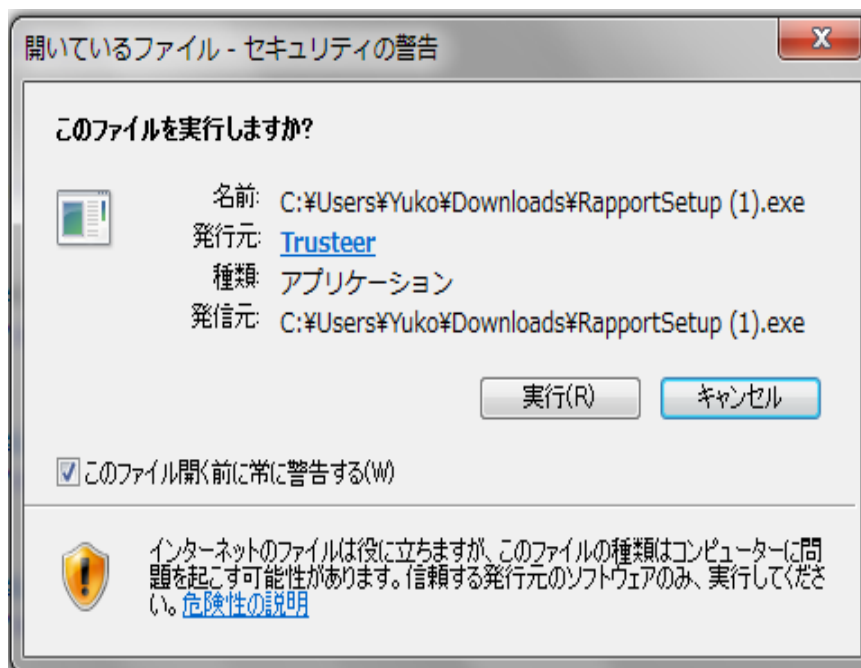
[もっと知る](#) [デモを見る](#) [後で実行する](#)

Trusteer

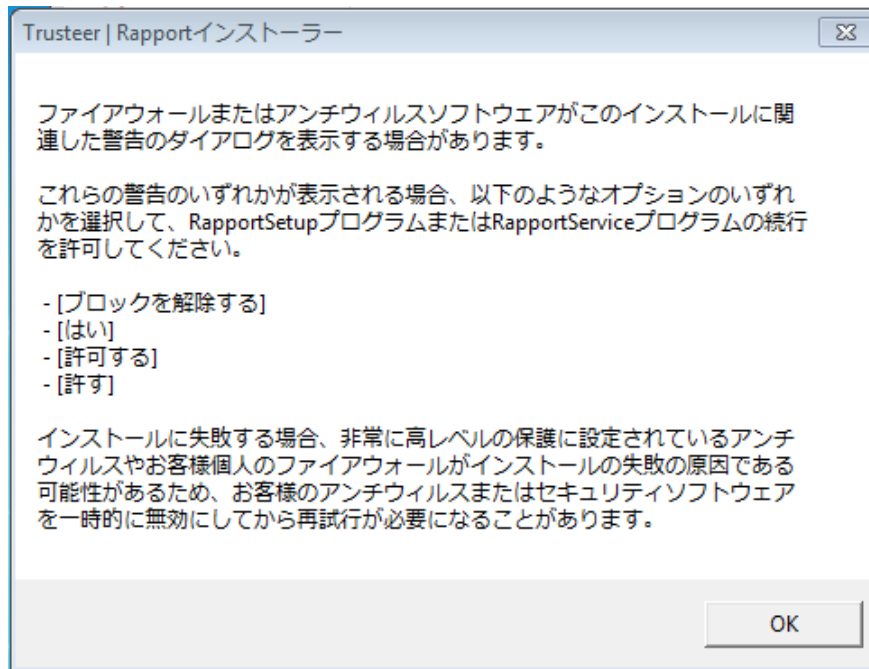
2. [ダウンロード]をクリックします。[セキュリティ警告 - ファイルをダウンロード]ダイアログボックスが表示され、RapportSetup.exeを実行するか、保存するかを尋ねられます。



3. [実行]をクリックします。数秒後、別のダイアログボックスが表示され、[このソフトウェアを起動しますか?]--と尋ねられます。



4. 再度**[実行]**をクリックします。以下のダイアログボックスが表示されます。



5. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

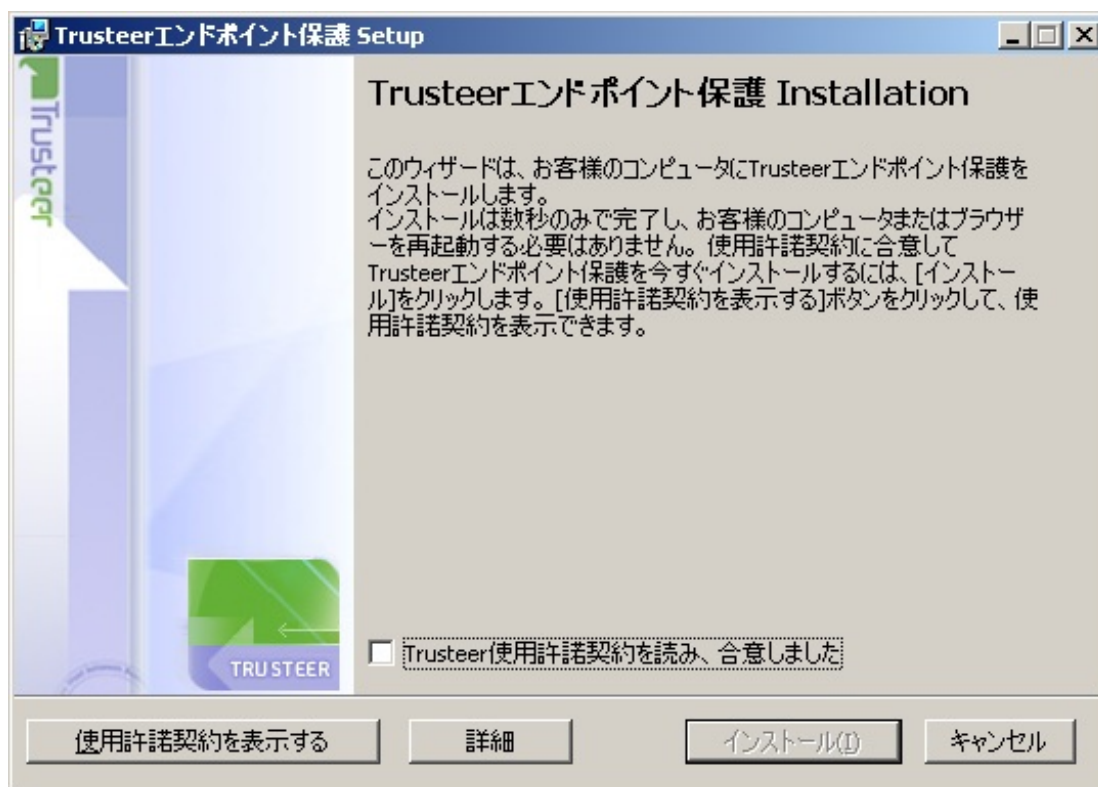
注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

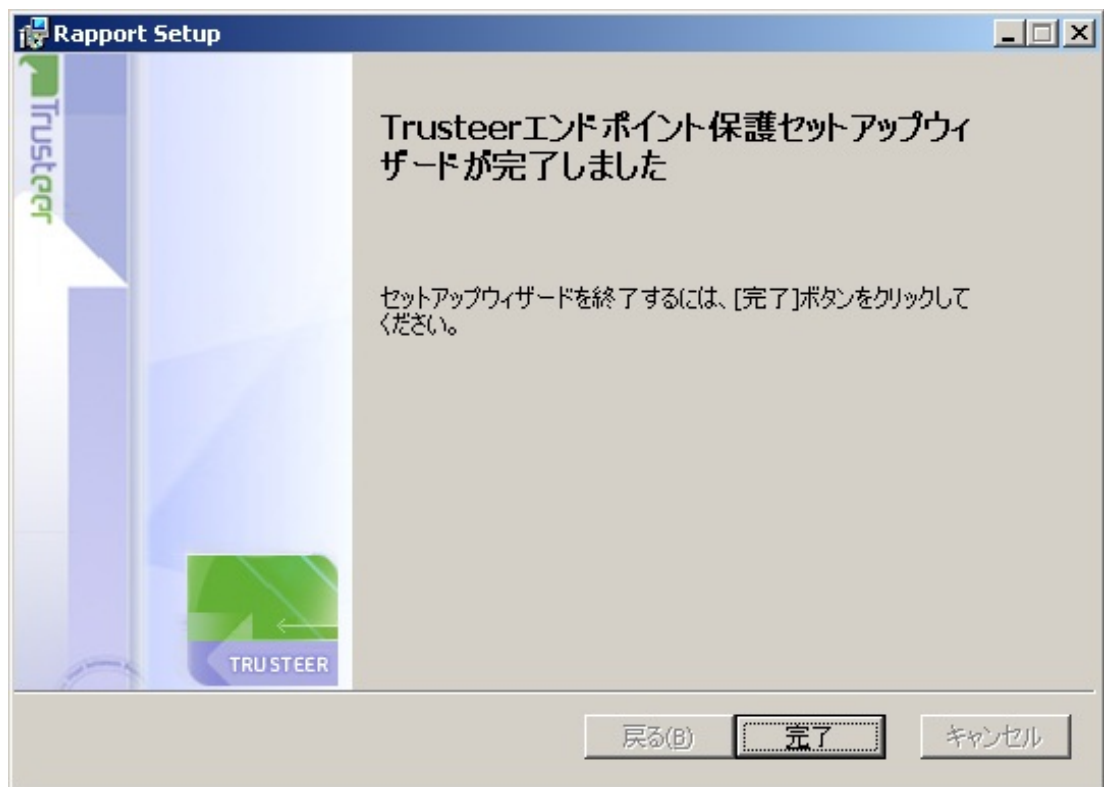
Rapportのインストールウィザードが表示されます。



- Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的を使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

7. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。
8. **[インストールする]**をクリックします。インストールが進行します。インストールが完了したら、ウィザードに**[終了する]**ボタンが表示されます。



9. **[終了する]**をクリックします。数秒後、新しいブラウザーウィンドウでTrusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザーでRapportのお礼ページが表示されます。

以上で、インストールは完了です。

Internet Explorer を使用した Windows XP への Trusteer Rapport のインストール

この手順では、Windows XP を実行しており、ブラウザーは Microsoft Internet Explorer を使用している場合の Trusteer Rapport のダウンロードおよびインストール方法を説明します。

➔ Trusteer Rapport のインストール方法

1. 組織のログインページをブラウズします。組織から Trusteer Rapport のダウンロードが提供されている場合は、[ダウンロード] ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。

御行のロゴはこちらへ

オンラインバンキング利用時に必須のセキュリティー

Trusteer Rapport をダウンロード

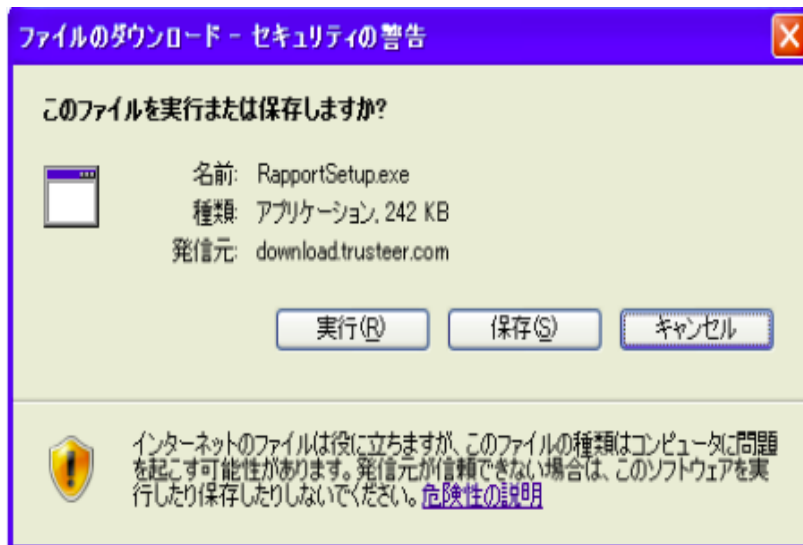
-  お客様の個人情報や銀行口座情報を、認証情報の盗難や詐欺から守ります。
-  各アンチウイルスソフトウェアと共存しながらも、それらのソフトウェアでは阻止できない攻撃からお客様を守ります。
-  効果的にお客様の環境を守る Trusteer Rapport は、簡単な使用方法で、お客様のコンピューターの減速を招くことはありません。

[今すぐダウンロード](#)

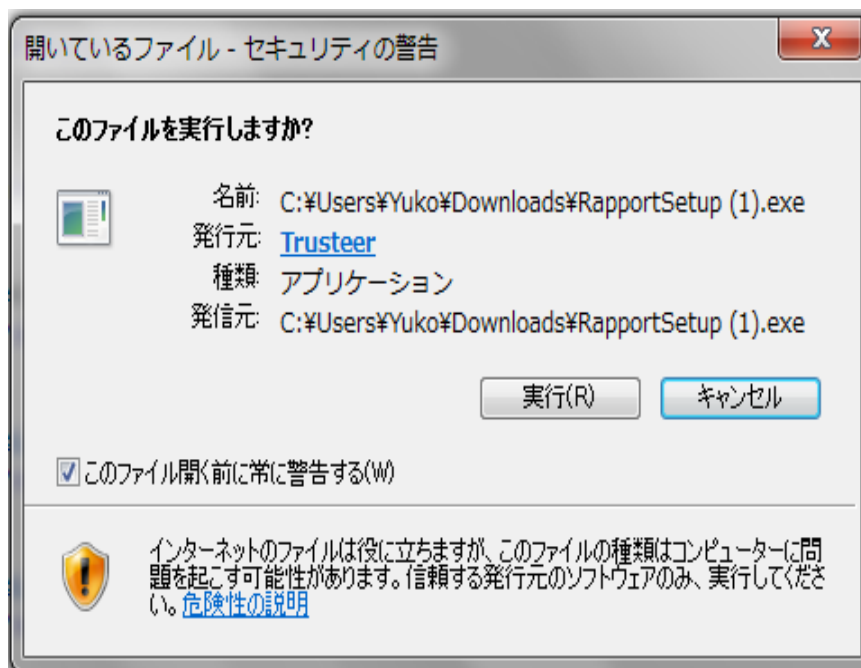
[もっと知る](#) [デモを見る](#) [後で実行する](#)

Trusteer

2. [ダウンロード]をクリックします。[セキュリティ警告 - ファイルをダウンロード]ダイアログボックスが表示され、RapportSetup.exeを実行するか、保存するかを尋ねられます。



3. [実行]をクリックします。数秒後、別のダイアログボックスが表示され、[このソフトウェアを起動しますか?]--と尋ねられます。



4. 再度**[実行]**をクリックします。以下のダイアログボックスが表示されます。



5. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

Rapportのインストールウィザードが表示されます。



- Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的地使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

7. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。
8. **[インストールする]**をクリックします。インストールが進行します。インストールが完了したら、ウィザードに**[終了する]**ボタンが表示されます。



9. [終了する]をクリックします。数秒後、新しいブラウザウィンドウで Trusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザでRapportのお礼ページが表示されます。

Trusteer

英語サイト | お問い合わせ | Search

製品 リソース 企業情報

インストールの完了 - OS X

Home » Support » インストールの完了 - OS X

技術サポート

FAQ

ビデオチュートリアル

弊社へのフィードバック

最も早く回答を探すには:
質問をここに入力し、以下に表示される回答を参照してください。

powered by nanoRep

Rapportをインストールしていただきありがとうございます!

Rapportを使用する理由

「最近行われた、業界トップクラスのアンチウイルスベンダーおよびウェブブラウザのアンチフィッシングフィルターに関するテストによると、インターネット上では過半数のアクティブなマルウェアおよびフィッシングの脅威が検知されておらず、平均検知率はマルウェアでは57%、フィッシングでは42%にとどまっています。」(Cyveillance社、2009年2月)

最近のマルウェアは、オンラインバンキング、証券取引、ショッピング、eコマース、電子メール、およびソーシャルネットワークウェブサイトにログイン認証情報を盗むことができます。ウェブサイトが「セキュア」であると見なされる場合でも、犯罪者はお客様のオンライン口座を使用して、不正なトランザクションの実行、発信、電子メールの送信、およびその他の操作を実行できます。

Trusteer Rapportは、スタンドアロンで使用することも、デスクトップセキュリティソリューションと併用することも可能です。Trusteer Rapportは、あらゆるタイプのマルウェアからお客様のログイン認証情報およびWeb通信を保護し、アカウントへの不正アクセスを防止します。ご使用のコンピューターで最新のアンチウイルスソリューションを実行している場合でも、Trusteer Rapportを使用する必要があります。

動作概要

Enterprise Login

サポートへのお問い合わせ

サポートチケットの送信

送付依頼

以上で、インストールは完了です。

Firefoxを使用したWindows 7へのTrusteer Rapportのインストール

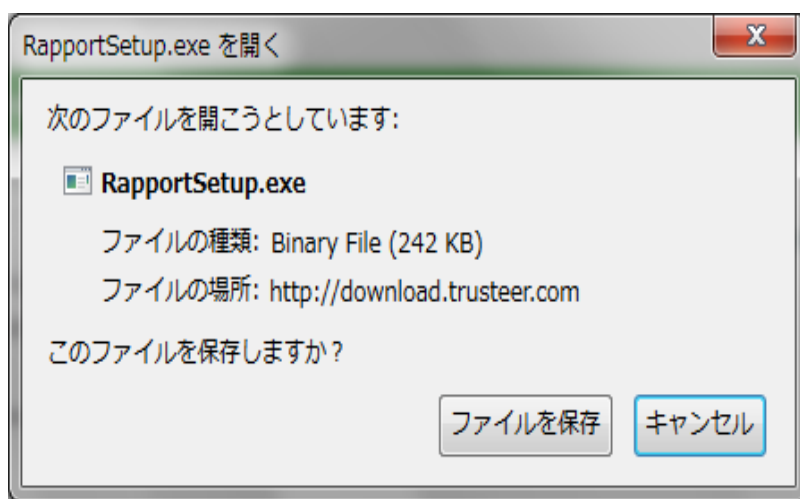
この手順では、Windows 7を実行しており、ブラウザはMozilla Firefoxを使用している場合のTrusteer Rapportのダウンロードおよびインストール方法を説明します。

→ Trusteer Rapportのインストール方法

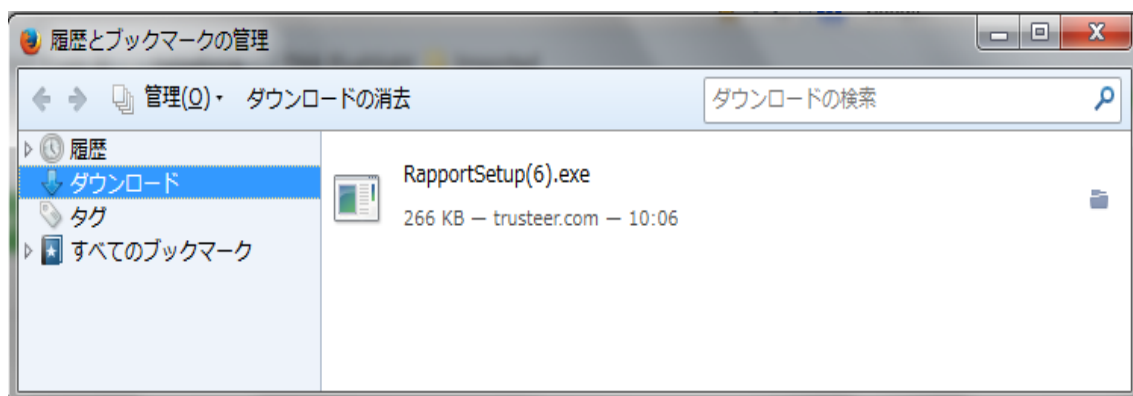
1. 組織のログインページをブラウズします。組織からTrusteer Rapportのダウンロードが提供されている場合は、[ダウンロード]ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。



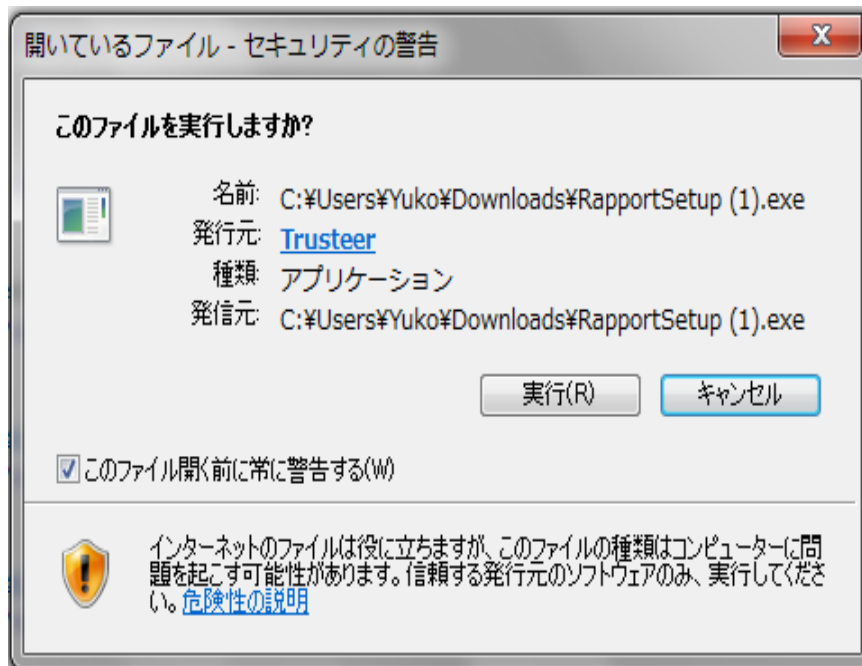
2. [ダウンロード]をクリックします。



3. [ファイルの保存]をクリックします。最近のダウンロードの一覧が表示されます。



4. リストの一番上に表示されているRapportSetup.exeファイルをダブルクリックします。セキュリティの警告が表示されます。

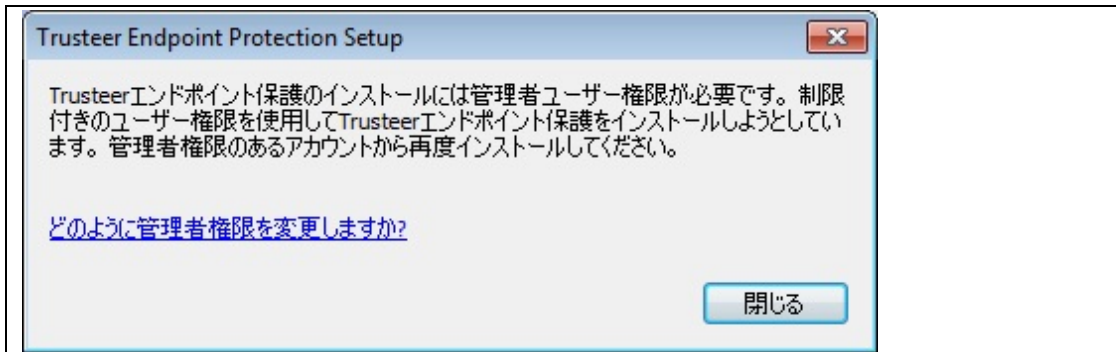


5. **[実行]**をクリックします。以下のダイアログボックスが表示されます。



6. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

Rapportのインストールウィザードが表示されます。

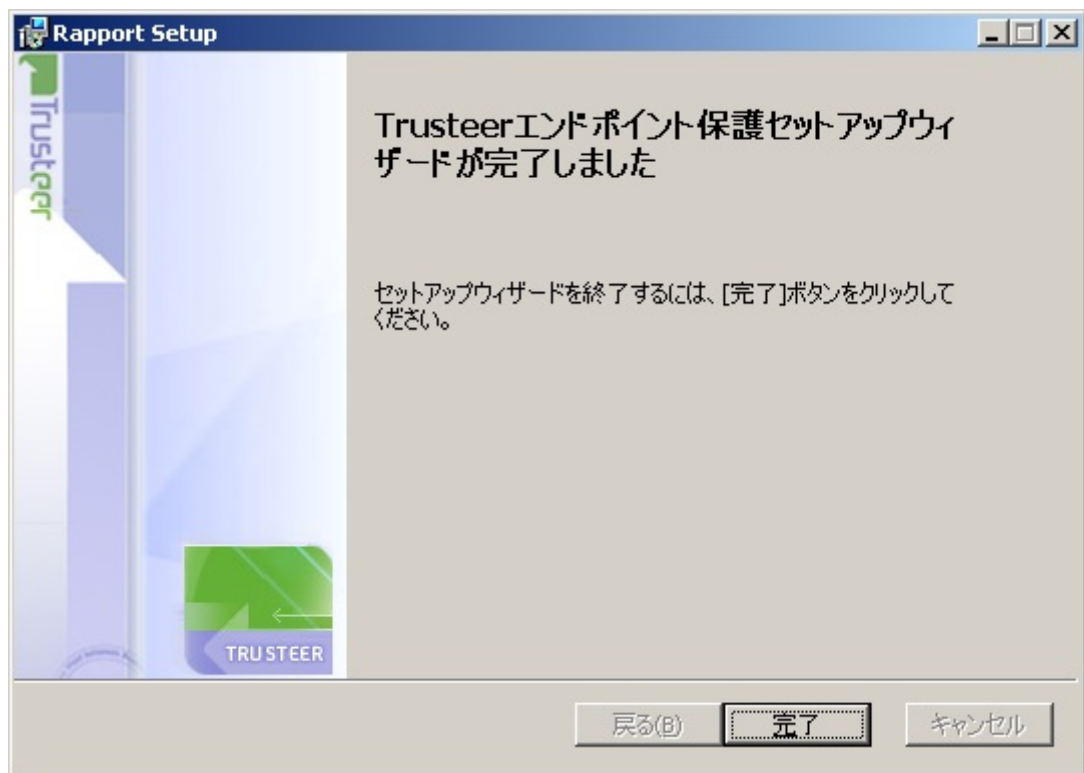


7. Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザーの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

8. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。

9. [インストールする]をクリックします。インストールが進行します。インストールが完了したら、ウィザードに[終了する]ボタンが表示されます。



10. [終了する]をクリックします。数秒後、新しいブラウザウィンドウで Trusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザでRapportのお礼ページが表示されます。

The screenshot shows the Trusteer Rapport installation completion page for OS X. The page has a clean, professional layout with a green and blue color scheme. At the top, there is a search bar and navigation links. The main content area features a green header with the text 'インストールの完了 - OS X'. Below this, there is a section titled 'Rapportを使用する理由' (Reasons to use Rapport) which discusses the benefits of the software, such as protecting against malware and phishing. There is also a '動作概要' (Operation Overview) section. The page includes a search bar, language selection flags, and an 'Enterprise Login' button.

以上で、インストールは完了です。

Google Chromeを使用したWindows 7へのTrusteer Rapport のインストール

この手順では、Windows 7を実行しており、ブラウザーはGoogle Chromeを使用している場合のTrusteer Rapportのダウンロードおよびインストール方法を説明します。

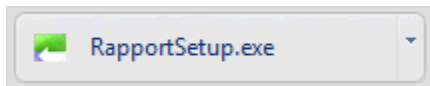
➔ Trusteer Rapportのインストール方法

1. 組織のログインページをブラウズします。組織からTrusteer Rapportのダウンロードが提供されている場合は、[ダウンロード]ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。

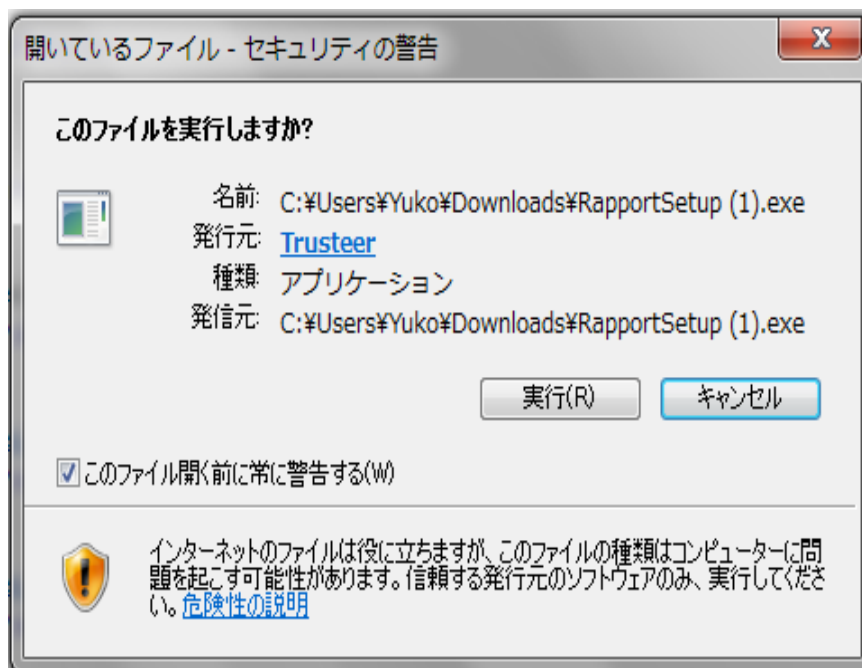


2. [ダウンロード]をクリックします。

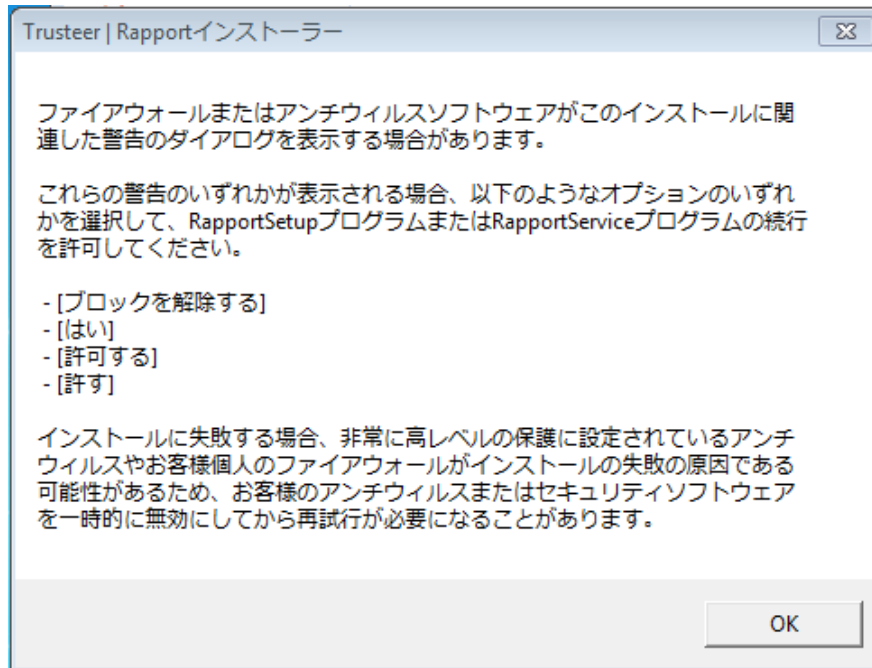
3. ブラウザーの設定に応じて、ブラウザーウィンドウの下部に、RapportSetup.exeをダウンロードするかどうかを尋ねるセキュリティメッセージが表示される場合があります。【保存する】をクリックします。ファイルがダウンロードされ、ブラウザーウィンドウの左下に、ダウンロードしたファイルの名前が表示されたボタンが表示されます。



4. ボタンをクリックします。ファイルを実行するかどうかを尋ねるセキュリティの警告が表示されます。



5. **[実行]**をクリックします。以下のダイアログボックスが表示されます。



6. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

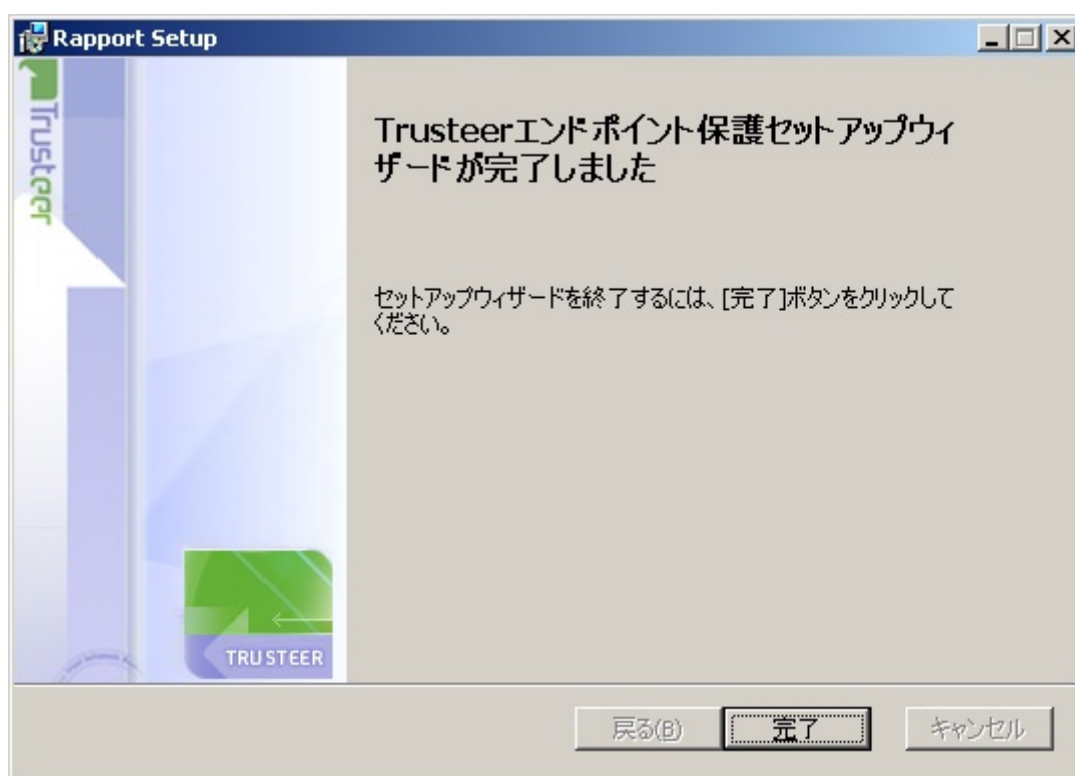
Rapportのインストールウィザードが表示されます。



- Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

8. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。
9. **[インストールする]**をクリックします。インストールが進行します。インストールが完了したら、ウィザードに**[終了する]**ボタンが表示されます。



- 10.[終了する]をクリックします。数秒後、新しいブラウザウィンドウで Trusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザでRapportのお礼ページが表示されます。

Trusteer

英語サイト | お問い合わせ | Search

製品 | リソース | 企業情報

インストールの完了 - OS X

Home > Support > インストールの完了 - OS X

技術サポート

FAQ

ビデオチュートリアル

弊社へのフィードバック

最も早く回答を探すには:
質問者ここに入力し、以下に表示される回答を参照してください。

Rapportをインストールしていただきありがとうございます! powered by nanoRep

Rapportを使用する理由

「最近行われた、業界トップクラスのアンチウイルスベンダーおよびウェブブラウザのアンチフィッシングフィルターに関するテストによると、インターネット上では過半数のアクティブなマルウェアおよびフィッシングの脅威が検知されておらず、平均検知率はマルウェアでは57%、フィッシングでは43%にとどまっています。」(Cyveillance誌、2009年2月)

最近のマルウェアは、オンラインバンキング、証券取引、ショッピング、eコマース、電子メール、およびソーシャルネットワークウェブサイトへのログイン認証情報を盗むことができます。ウェブサイトが「セキュア」であると見なされる場合でも、犯罪者はお客様のオンライン口座を使用して、不正なトランザクションの実行、発信、電子メールの送信、およびその他の操作を実行できます。

Trusteer Rapportは、スタンドアロンで使用することも、デスクトップセキュリティソリューションと併用することも可能です。Trusteer Rapportは、あらゆるタイプのマルウェアからお客様のログイン認証情報およびWeb通信を保護し、アカウントへの不正アクセスを防止します。ご使用のコンピューターで悪質なアンチウイルスソリューションを実行している場合でも、Trusteer Rapportを使用する必要があります。

動作概要

Enterprise Login

サポートへのお問い合わせ

サポートチケットの送信

送信履歴

以上で、インストールは完了です。

Firefoxを使用したWindows XPへのTrusteer Rapportのインストール

この手順では、Windows XPを実行しており、ブラウザはMozilla Firefoxを使用している場合のTrusteer Rapportのダウンロードおよびインストール方法を説明します。

→ Trusteer Rapportのインストール方法

1. 組織のログインページをブラウズします。組織からTrusteer Rapportのダウンロードが提供されている場合は、[ダウンロード]ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。

御行のロゴはこちらへ

オンラインバンキング利用時に必須のセキュリティー

Trusteer Rapport をダウンロード

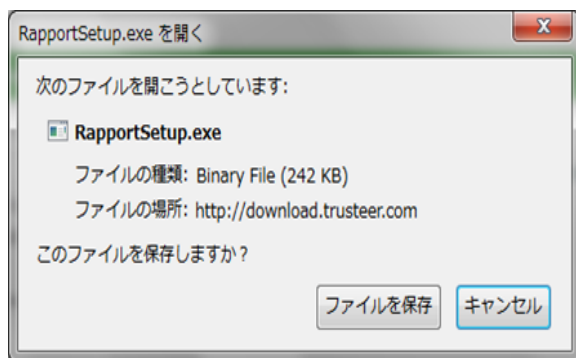
-  お客様の個人情報や銀行口座情報を、認証情報の盗難や詐欺から守ります。
-  各アンチウイルスソフトウェアと共存しながらも、それらのソフトウェアでは阻止できない攻撃からお客様を守ります。
-  効果的にお客様の環境を守る Trusteer Rapport は、簡単な使用方法で、お客様のコンピューターの減速を招くことはありません。

[今すぐダウンロード](#)

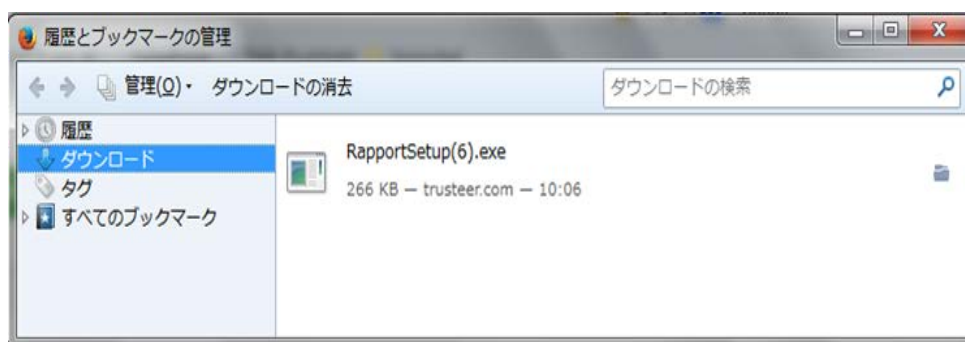
[もっと知る](#) [デモを見る](#) [後で実行する](#)

Trusteer

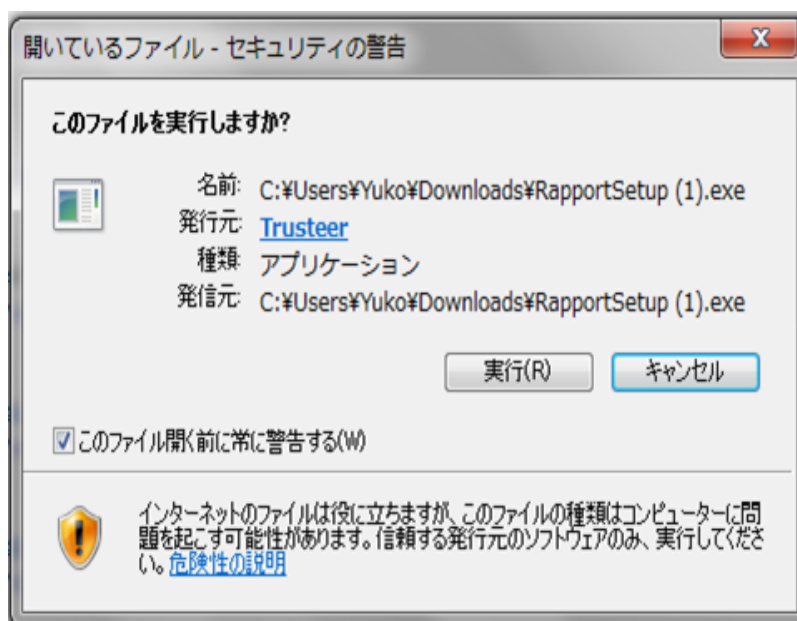
2. [ダウンロード]をクリックします。



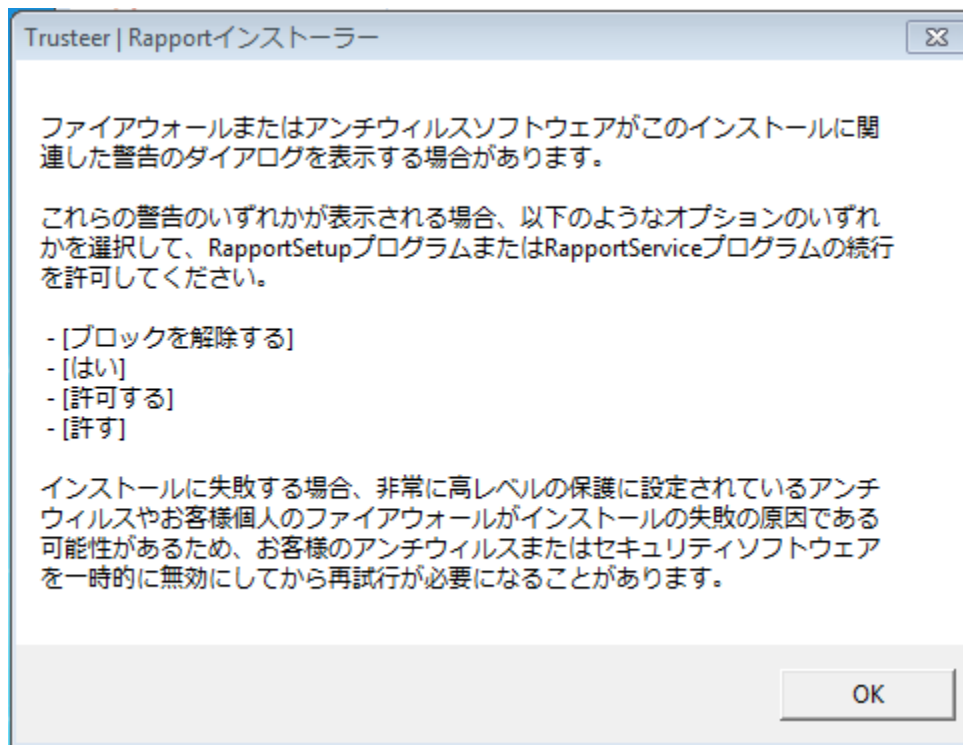
3. [ファイルの保存]をクリックします。最近のダウンロードの一覧が表示されます。



4. リストの一番上に表示されているRapportSetup.exeファイルをダブルクリックします。セキュリティの警告が表示されます。



5. **[実行]**をクリックします。以下のダイアログボックスが表示されます。



6. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

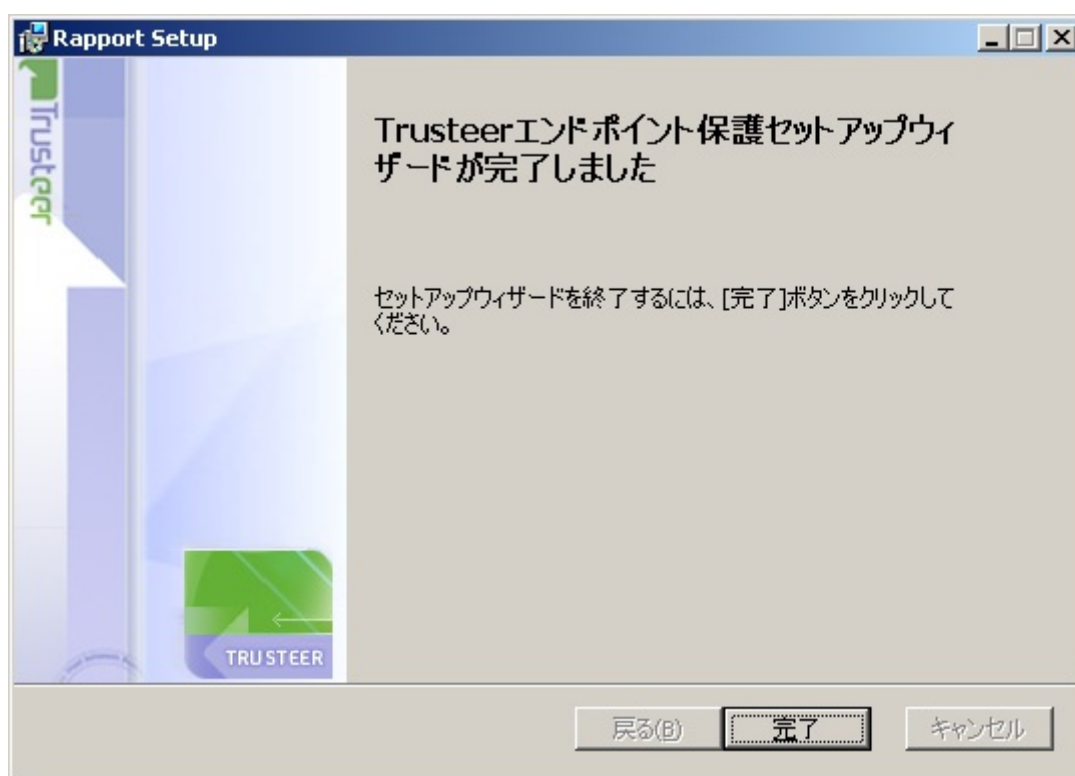
Rapportのインストールウィザードが表示されます。



- Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

8. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。
9. **[インストールする]**をクリックします。インストールが進行します。インストールが完了したら、ウィザードに**[終了する]**ボタンが表示されます。



10. [終了する]をクリックします。数秒後、新しいブラウザウィンドウで Trusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザでRapportのお礼ページが表示されます。

Trusteer 英語サイト | お問い合わせ | Search

製品 リソース 企業情報

インストールの完了 - OS X

Home » Support » インストールの完了 - OS X

技術サポート

FAQ

ビデオチュートリアル

弊社へのフィードバック

最も早く回答を探すには:
質問書にここを入力し、以下に表示される回答を参照してください。

powered by nanoRep

Rapportをインストールしていただきありがとうございます!

Rapportを使用する理由

「最近行われた、業界トップクラスのアンチウイルスベンダーおよびウェブブラウザのアンチフィッシングフィルターに関するテストによると、インターネット上では過半数のアクティブなマルウェアおよびフィッシングの脅威が検知されておらず、平均検知率はマルウェアでは57%、フィッシングでは43%にとどまっています。」(Cyveillance誌、2009年2月)

最近のマルウェアは、オンラインバンキング、証券取引、ショッピング、eコマース、電子メール、およびソーシャルネットワークウェブサイトへのログイン認証情報を盗むことができます。ウェブサイトが「セキュア」であると見なされる場合でも、犯罪者はお客様のオンライン口座を使用して、不正なトランザクションの実行、発信、電子メールの送信、およびその他の操作を実行できます。

Trusteer Rapportは、スタンドアロンで使用することも、デスクトップセキュリティソリューションと併用することも可能です。Trusteer Rapportは、あらゆるタイプのマルウェアからお客様のログイン認証情報およびWeb通信を保護し、アカウントへの不正アクセスを防止します。ご使用のコンピューターで悪質なアンチウイルスソリューションを実行している場合でも、Trusteer Rapportを使用する必要があります。

動作概要

以上で、インストールは完了です。

Google Chrome を使用した Windows XP への Trusteer Rapport のインストール

この手順では、Windows XP を実行しており、ブラウザーは Google Chrome を使用している場合の Trusteer Rapport のダウンロードおよびインストール方法を説明します。

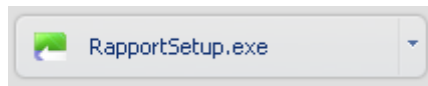
➔ Trusteer Rapport のインストール方法

1. 組織のログインページをブラウズします。組織から Trusteer Rapport のダウンロードが提供されている場合は、[ダウンロード] ボタンが表示されたスプラッシュスクリーンが表示されます。以下はその例です。

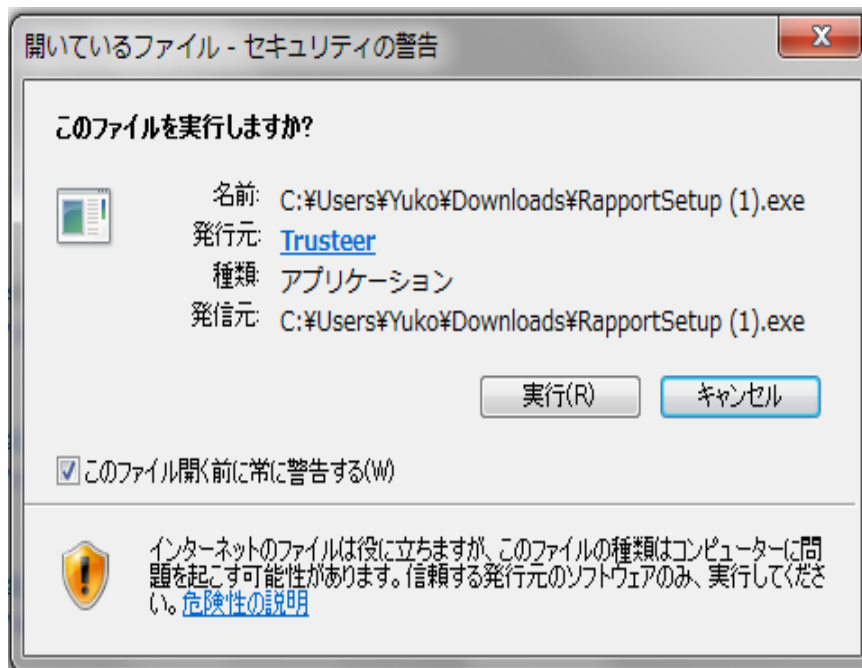


2. [ダウンロード] をクリックします。

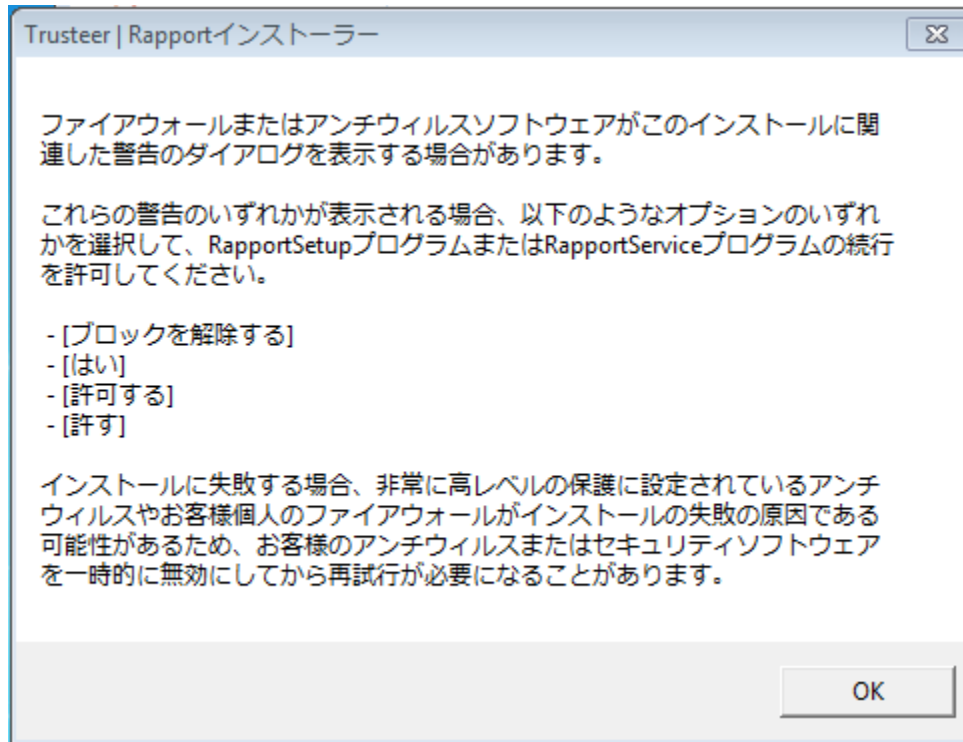
3. ブラウザーの設定に応じて、ブラウザーウィンドウの下部に、RapportSetup.exeをダウンロードするかどうかを尋ねるセキュリティメッセージが表示される場合があります。【保存する】をクリックします。ファイルがダウンロードされ、ブラウザーウィンドウの左下に、ダウンロードしたファイルの名前が表示されたボタンが表示されます。



4. ボタンをクリックします。ファイルを実行するかどうかを尋ねるセキュリティの警告が表示されます。



5. **[実行]**をクリックします。以下のダイアログボックスが表示されます。



6. **[OK]**をクリックします。Trusteer Rapportがダウンロードされます。

注: この時点で、以下のメッセージが表示される場合があります。



これは、ご利用のプロバイダーでは、Windowsの標準ユーザーアカウントからTrusteer Rapportをインストールすることが許可されていないことを意味します。このメッセージが表示されたら、管理者アカウントに切り替えてから、再度インストールを実行してください。

管理者アカウントへの切り替え方法

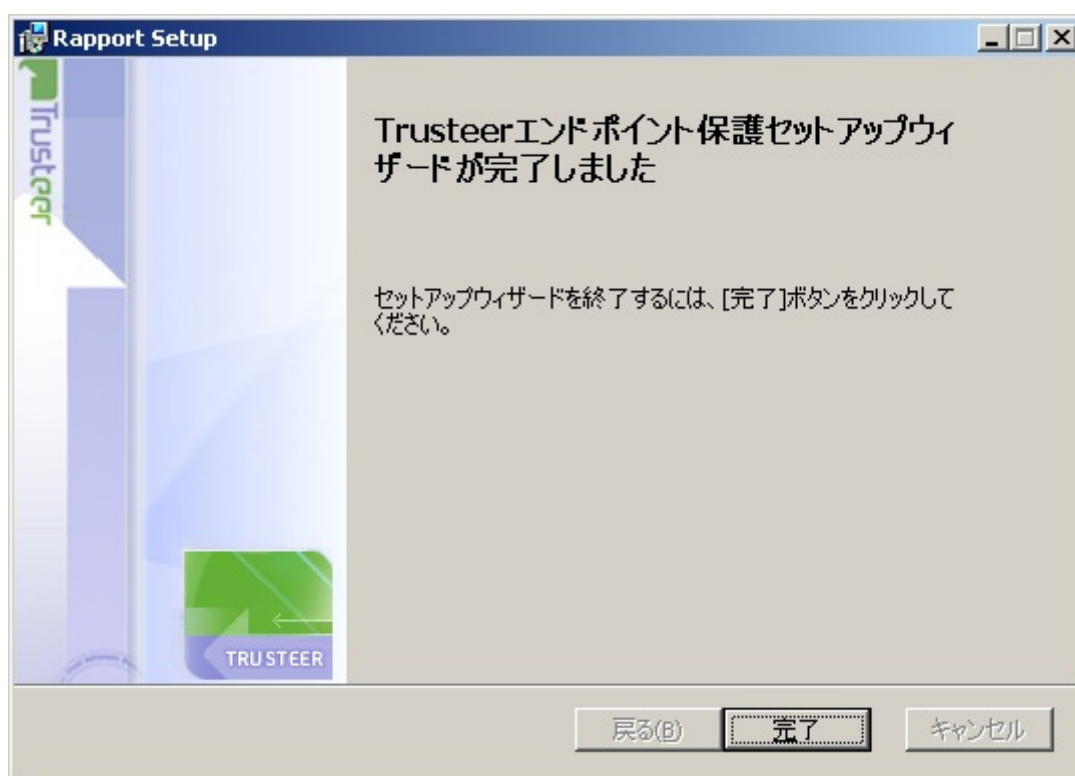
Rapportのインストールウィザードが表示されます。



- Trusteer Rapportを読み上げソフト対応にする必要がある場合は、**[詳細]**をクリックします。詳細オプション画面が表示されます。**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしてから、**[続行する]**をクリックします。こうすることで、互換性のある読み上げソフトによるTrusteer Rapportのメニューおよびダイアログの読み上げが可能になり、Trusteer Rapportにより、ブラウザの内容の読み上げが防止されることがなくなります。また、Rapportの停止またはアンインストールなどのいくつかのアクションで必要とされる、Trusteer Rapportの停止またはアンインストールが実行されたときに表示される、視覚コードチャレンジのセキュリティダイアログも無効になります。

注: 読み上げソフトを使用する必要があるコンピューターにTrusteer Rapportをインストールする場合以外は、**[私には視覚障害があり、画面読み上げ支援技術を定期的に使用します]**チェックボックスをオンにしないでください。この設定により、一部のセキュリティ機能が無効になります。

8. **[Trusteer使用許諾契約を読み、合意しました]**をオンにします。
9. **[インストールする]**をクリックします。インストールが進行します。インストールが完了したら、ウィザードに**[終了する]**ボタンが表示されます。



- 10.[終了する]をクリックします。数秒後、新しいブラウザウィンドウで Trusteer Rapportが開き、短時間の互換性テストが実行されます。テストが完了すると、Trusteer Rapportにより、ブラウザでRapportのお礼ページが表示されます。

The screenshot shows the Trusteer Rapport installation completion page for OS X. The page has a clean, professional layout with a green and blue color scheme. At the top, there is a search bar and navigation links. The main content area features a green header with the text 'インストールの完了 - OS X'. Below this, there is a search box and a section titled 'Rapportを使用する理由' (Reasons to use Rapport). The text in this section discusses the benefits of Rapport, such as its ability to detect and prevent malware infections. There is also a '動作概要' (Operation Overview) section. On the right side, there are language selection flags and an 'Enterprise Login' button. The overall design is modern and user-friendly.

以上で、インストールは完了です。

Windows Server (2003または2008)へのTrusteer Rapportのインストール

Trusteer Rapportは、Windows Server (2003または2008)へのインストールをサポートしています。また、Trusteer Rapportは複数のユーザーセッションをサポートしています。Trusteer Rapportを1つインストールするだけで、共有仮想デスクトップ環境では必要とされる、複数のプロファイルに対応することができます。Trusteer Rapportは、Windows Server (2003または2008)でインストールプロセスを実行すると、これを検知し、サーバーバージョンをインストールします。サーバーバージョンには、1人のユーザーがシステム上で実行されているすべてのユーザーのシステムを再起動してしまう状況を回避するため、ユーザーへの再起動要求の送信が無効になっています。再起動要求の無効化の詳細情報については、『Trusteer Rapport Virtual Environment Best Practices』を参照してください。

➔ Windows Server 2003または2008へのTrusteer Rapportのインストール方法

1. RapportSetup.exeファイルを実行します。このファイルの標準バージョンは、<http://www.trusteer.com/support/rapport-installation-links>で入手できます。企業のお客様の場合、この設定ファイルのカスタマイズバージョンを、Trusteerプロジェクトマネージャーから入手できます。

2. インストールパッケージ一式をダウンロードし、インストールウィザードを開始するインストールプロセスを実行します。インストールウィザードによりサーバーOSが検知され、**[Windows Serverを検出]**画面が表示されます。

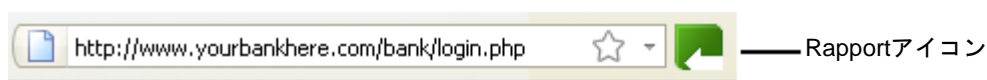


3. この画面が表示されたら、**[ドキュメントを表示する]**をクリックします。ご使用のWebブラウザーに、Trusteer Rapportがどのように企業の保護に役立つかを説明した[Trusteer Rapportの企業サポートページ](#)が表示されます。弊社では、この企業サポートで『Trusteer Rapport Virtual Implementation Scenarios』へのリンクをクリックしてこの文書を一読することをお奨めしています。この文書には、Trusteer Rapportを仮想デスクトップ環境で実装するうえでの重要な情報が記載されています。
4. 文書を読み終えたら、**[ドキュメントを読みました]**チェックボックスをオンにして、インストールを続行します。

[Windows Serverを検出]画面以外は、インストール方法はその他のオペレーティングシステムと全く同じです。

4. アプリケーションの開始

インストールが完了すると、Trusteer Rapportがただちに実行され、ユーザーとパートナーWebサイト間の通信の保護が開始されます。ブラウザのアドレスバー上または右端に、Trusteer Rapportのアイコンが表示されます。銀行または企業のWebサイトをブラウズすると、Trusteer Rapportのアイコンが緑色になり、サイトが保護されていることが示されます。



インストール後初めてオンライン口座にログインすると、[「パスワード保護の提示に対する応答」](#) (107ページ)で説明されているように、パスワード保護が提示されます。

Trusteer Rapportで保護されていないWebサイトをブラウズすると、Rapportのアイコンは灰色になります。灰色のアイコンをクリックすると、ドロップダウンダイアログボックス([Rapportステータスインジケーター])が表示され、そのサイトが保護されていないことが通知されます。



以下のように操作します。

- ログインしたり、機密情報を表示または送信したりするWebサイトを、追加で保護します。
- [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。本書に記載されている多くの手順では、まずコンソールを開くことから始めています。

- 関心のある情報についてのトピックの見出しに目を通します。
- インターネットを介した業務の実行、バンキング、およびショッピングで、より高い安全性を感じるできるようになります。

追加のWebサイト保護

注: 一部のTrusteer Rapportのインストールでは、この機能が無効になっています。

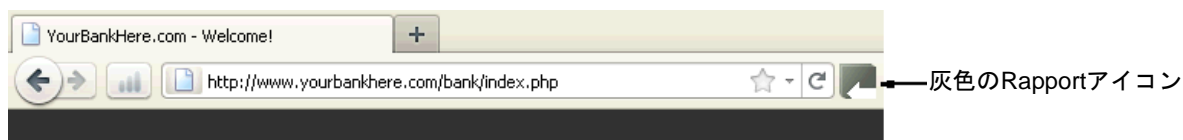
デフォルトでは、Trusteer Rapportは、ユーザーにTrusteer Rapportを提供した組織などの、パートナーWebサイトを保護しています。弊社のパートナーは、顧客に対してTrusteer Rapportのインストールを推奨しています。しかし、すべての銀行およびその他の企業がTrusteerと連携しているわけではありません。

ユーザーは、簡単な操作でTrusteer Rapportの保護を追加のWebサイトに拡張することができます。保護できるWebサイトの数に制限はありません。Trusteerは、ユーザーが個人情報や、あらゆる種類の機密情報をやりとりするすべてのWebサイトに対して、追加でTrusteer Rapportの保護をアクティブにすることをお奨めしています。ユーザーが保護すべきWebサイトには、たとえば以下のようなサイトが含まれます。

- オンライン銀行口座
- ミューチュアルファンド口座
- オンライン証券取引口座
- オンライン商取引
- Webベース電子メールサイト(Hotmail、Yahoo!メール、Gmailなど)
- ソーシャルネットワーキングサイト(Myspace、Orkut、Linkedinなど)
- 保険契約申し込み
- 個人の医療情報サイト
- オンライン商取引(eBay、Amazon、Walmart.com、Target.comなど)

➔ 追加のWebサイト保護方法

1. 保護するWebサイトをブラウザします。このWebサイトではまだTrusteer Rapportによる保護が有効になっていない場合、アドレスバーに表示されるアイコンは灰色です。



YourBankHere

> [Login to my account](#) > [Create new account](#) > [Support](#)

2. アドレスバーで、灰色のRapportアイコンをクリックします。ドロップダウンダイアログボックスが表示されます。



3. ドロップダウンダイアログボックスで、[このWebサイトを保護する]をクリックします。アドレスバーに表示されているRapportのアイコンが緑色に変わり、このWebサイトがTrusteerによって保護されていることが示されます。



このアイコンは、デフォルトで表示されます。 [「Trusteer Rapportのアドレスバーアイコンの表示/非表示」](#) (160ページ)の説明に従って、Trusteer Rapportのアドレスバーアイコンの表示/非表示を選択できます。

Trusteer Rapportアイコンがブラウザーに表示されない場合

Trusteer Rapportアイコンがブラウザーに表示されない理由としては、以下が考えられます。

- アドレスバーでアイコンを非表示にするように選択しています。アイコンは非表示でも、Trusteer Rapportによる保護は提供されています。アイコンは、元に戻すことができます。Trusteer Rapportアイコンの表示/非表示の切り替えの詳細については、[「Trusteer Rapportのアドレスバーアイコンの表示/非表示」](#) (160ページ)を参照してください。
- Trusteer Rapportは、ご使用のブラウザーをサポートしていません。現在サポートされているブラウザーの一覧については、<http://www.trusteer.com/support/faq/supported-platforms>を参照してください。
- Trusteer Rapportが停止され、稼働していません。Trusteer Rapportは再度起動できます。[「Trusteer Rapportの起動」](#) (209ページ)を参照してください。

Rapportコンソールのオープン


Trusteer Rapportコンソールは、さまざまなTrusteer Rapportの機能および情報へのポータルです。

➔ Rapportコンソールを開く方法

- システムトレイで、Trusteer Rapportアイコン(🔒)をクリックします。
Rapportコンソールが表示されます。



システムトレイにRapportアイコンが表示されていない場合

デフォルトでは、Rapportシステムトレイアイコン()は、Trusteer Rapportが実行されている間、表示されています。このアイコンは、非表示にすることができます([「Trusteer Rapportのアドレスバーアイコンの表示/非表示」](#) (162ページ)を参照してください)。このアイコンは、Trusteer Rapportのブラウザーに依存しない保護が機能していることを示しています。これには、マルウェアの防止、スキャン、駆除が含まれます。Rapportコンソールで非表示にしていなくてもかかわらず、このアイコンが表示されていない場合は、Trusteer Rapportは実行されていません。Trusteer Rapportが停止されたか、アンインストールされた可能性があります。Trusteer Rapportが停止されている場合、これを起動するには、**[すべてのプログラム] > [Trusteer Rapport] > [スタート]**を選択してください。

5. オンラインバンキングの保護

ご利用の銀行がTrusteer Rapportのパートナーである場合、銀行のWebサイトからTrusteer Rapportをダウンロードできます。Trusteer Rapportをインストールし次第、完全に保護されたオンラインバンキングを利用することができます。

Trusteer Rapportはセキュリティの危険性を特定し、ユーザーに通知せずにその脅威を無効にします。Trusteer Rapportが一定のレベル以上のリスクを検知した場合、Rapportは脅威を無効化する前に、ユーザーの確認を促すことがあります。Trusteer Rapportのアラートおよび警告への応答に関する詳細については、[「アラートおよび警告への応答」](#) (92ページ)を参照してください。

6. 企業 Web サイトの保護

Webを介して会社のネットワークや企業ポータルにアクセスする場合、コンピュータにTrusteer Rapportをインストールしておく、ユーザー自身のIDを保護し、ユーザーの認証情報を悪用した企業へのセキュリティ侵害の回避に役立ちます。Trusteer Rapportのパートナー企業に所属しているユーザーの場合、Trusteer Rapportをインストールすると、ただちに企業Webサイトへのアクセスの保護が開始されます。

Trusteer Rapportはセキュリティの危険性を特定し、ユーザーに通知せずにその脅威を無効にします。Trusteer Rapportが一定のレベル以上のリスクを検知した場合、Rapportは脅威を無効化する前に、ユーザーの確認を促すことがあります。Trusteer Rapportのアラートおよび警告への応答に関する詳細については、[「アラートおよび警告への応答」](#) (92ページ)を参照してください。

7. オンラインでの安全なクレジットカードの使用

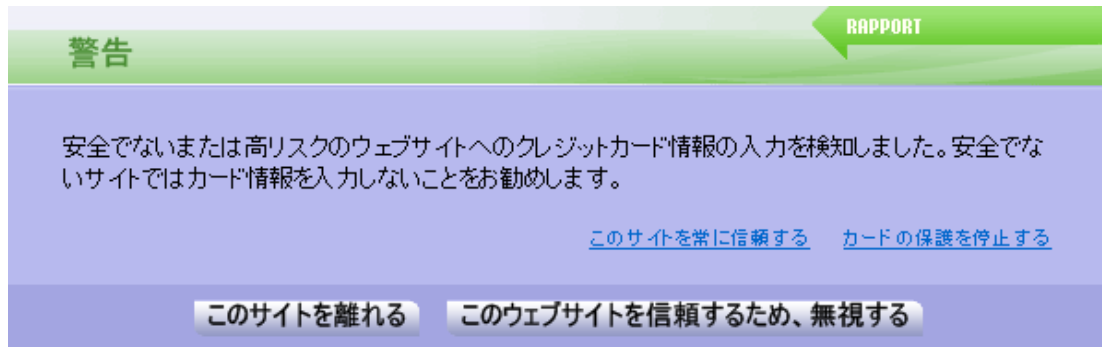
Trusteer Rapportは、クレジットカードをオンラインで使用する際に、クレジットカード情報の盗難からユーザーを保護します。

Trusteer Rapportは、登録しているカード会社によって発行されたクレジットカードに対して、以下の保護機能を提供しています。

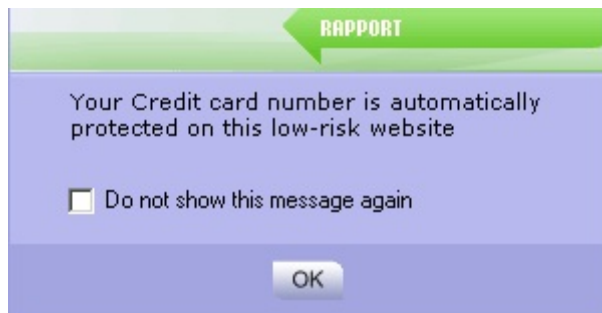
- ユーザーが登録しているカード会社のBIN (Bank Identification Number: 銀行識別コード)をWebページに入力すると、これを検知します。
- ユーザーがBINを入力すると、ただちにキーロガーブロック機能をアクティブにし、キーロギングマルウェアにより、クレジットカード番号が読み取られないようにします。
- キーロガーブロック機能がアクティブになったら、ユーザーに通知します。
- 疑わしい、または安全でないWebサイトでユーザーがクレジットカード番号を入力した場合、ユーザーにアラートを通知して、ユーザーがそのサイトを信頼するか、クレジットカード番号の送信を中止するかを選択できるようにしています。

注: Trusteer Rapportがユーザー個人のクレジットカード番号を知ることはありません。Trusteer Rapportは、カード発行会社を識別するカード番号の最初の数桁の番号を認識します。これは、銀行識別コード(BIN)と呼ばれています。

クレジットカード番号を入力すると、以下のいずれかのメッセージが表示されます。



この警告の詳細については、[「クレジットカード情報送信検知の警告に対する応答」](#) (129ページ)を参照してください。



このメッセージの詳細については、[「クレジットカード保護のメッセージに対する応答」](#) (131ページ)を参照してください。

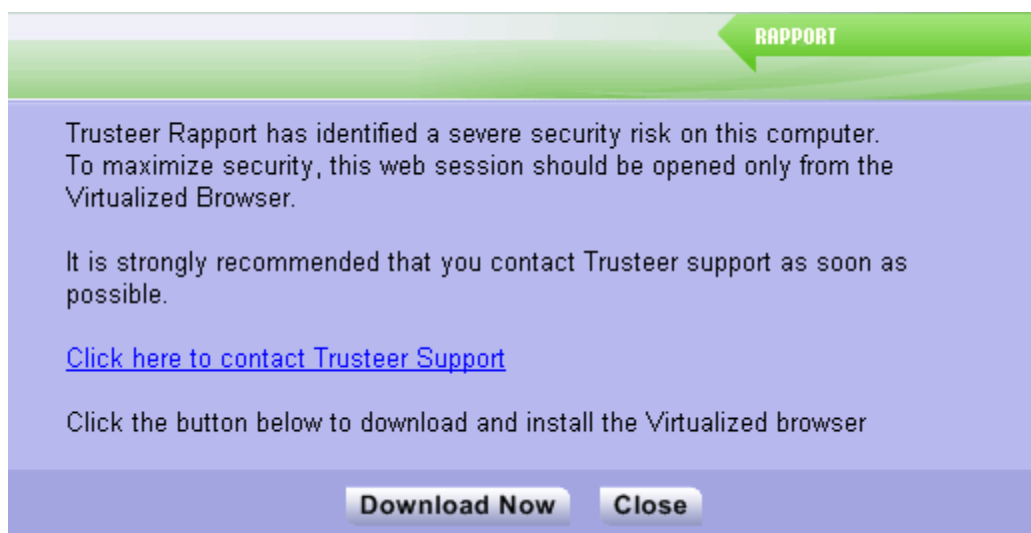
8. Trusteer Rapport の仮想化ブラウザの使用

Trusteer Rapportの仮想化ブラウザは、保護されたWebサイトをブラウズする際に、追加の保護レイヤーを提供するものです。この保護レイヤーでは、コンピューターに潜んでいる可能性のある悪意のあるソフトウェアから保護するために、隔離されたブラウジング環境が構築されます。

Trusteer Rapportは、以下のような状況において、仮想化ブラウザのダウンロードを提供します。

- ユーザーが保護されたWebサイトをブラウズしたときに、Trusteer Rapportにより、使用しているコンピューターに深刻なセキュリティリスクが存在することが検知された場合。この場合、Trusteer Rapportにより、通常のブラウザでそのサイトを開くことが阻止されます([「仮想化ブラウザの強制ダウンロードアラートに対する応答」](#) (92)ページを参照)。
- 仮想化ブラウザを使用したオプション表示がサポートされているサイトをブラウズした場合([「仮想化ブラウザのオプションダウンロードアラートに対する応答」](#) (95)ページを参照)。

ダウンロードの提供には、[ダウンロード]ボタンが表示されます。以下はその例です。



➔ 仮想化ブラウザのインストール方法

1. 仮想化ブラウザのダウンロード提供が表示されたら、[ダウンロード] ボタンをクリックします。ご使用のブラウザに、以下のWebページが表示されます。

Trusteer

英語サイト | お問い合わせ |

製品

リソース

企業情報

Trusteer Rapport 仮想化ブラウザ インストール

Home , Support , Trusteer Rapport 仮想化ブラウザ インストール-64

Technical Support

FAQ

Video Tutorials

Send us your feedback!

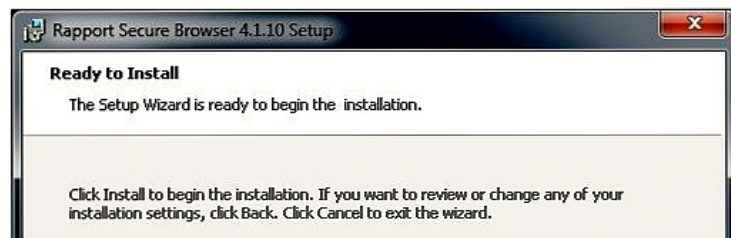
To download the Trusteer Rapport Virtualized Browser, click here.

Trusteer Rapport仮想化ブラウザをダウンロードするには、ここをクリックしてください。

仮想化ブラウザをインストールするには、Trusteer Rapportがすでにコンピューターにインストールされている必要があります。

仮想化ブラウザのインストール方法

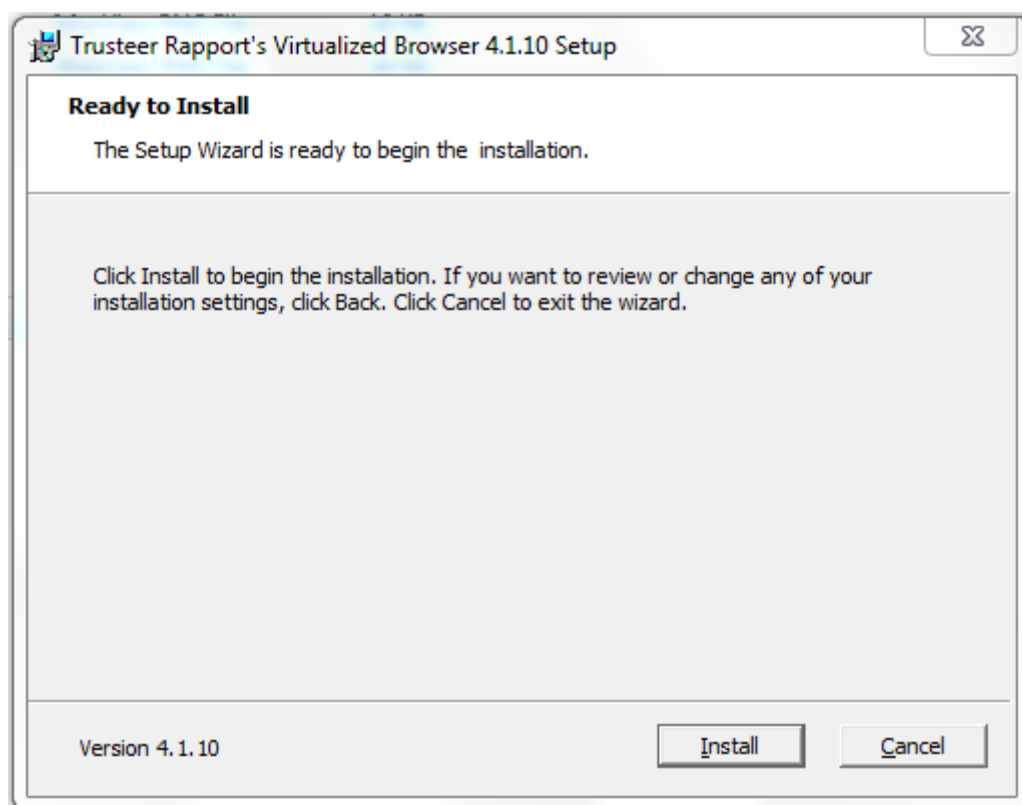
1. インストールファイルをダブルクリックします。Trusteer Rapport仮想化ブラウザ設定ウィザードのウィンドウが開きます。



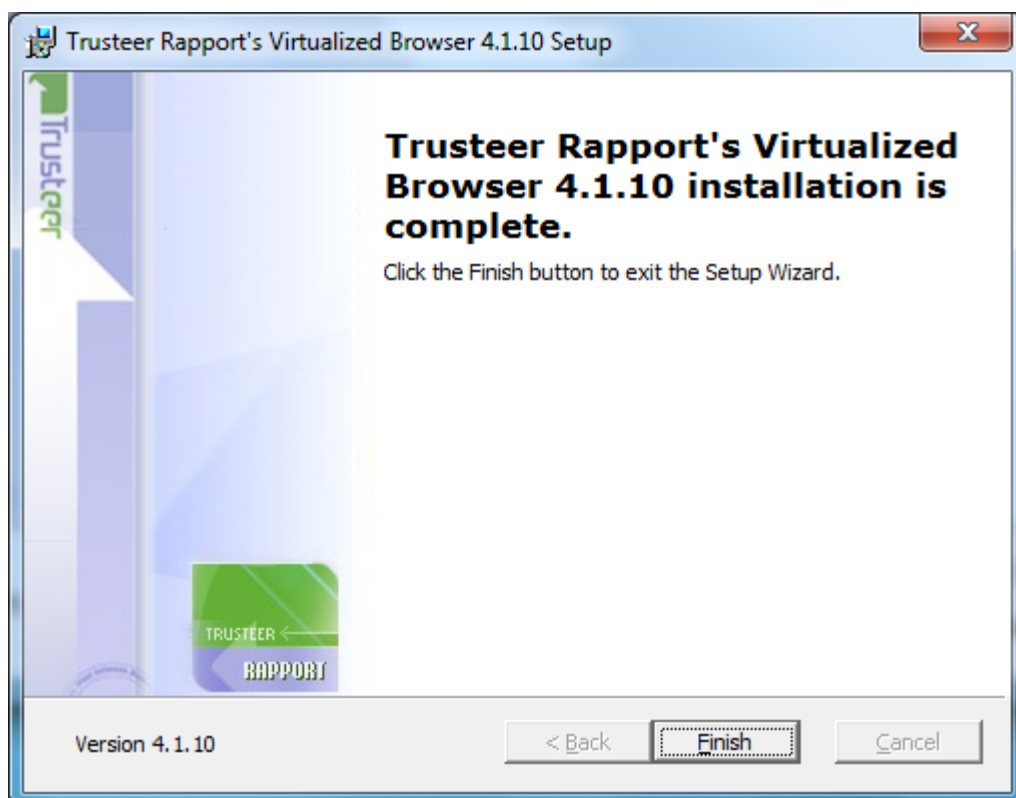
2.

3. [here] リンクをクリックします。ご使用のブラウザで、VirtualizedBrowserSetup.exeのダウンロードが開始されます。

4. VirtualizedBrowserSetup.exeのダウンロードが完了したら、ファイルを実行します。設定ウィザードで仮想化ブラウザをインストールできる状態になったら、以下の画面が表示されます。



5. [インストールする]をクリックします。インストールプロセスが開始されます。インストールが完了すると、以下の画面が表示されます。



6. [終了する]をクリックします。以上で、仮想化ブラウザーがインストールされました。これで、ダウンロードが提供されたときに開こうとしていたWebサイトを開くことができます。別のアラートが表示され、そのサイトを仮想化ブラウザーで開くことが促されます。[「仮想化ブラウザーのオプションダウンロードアラートに対する応答」](#) (95ページ)または[「仮想化ブラウザーのオプションアラートに対する応答」](#) (101ページ)を参照してください。

9. Trusteer Rapport のセキュアソフトトークンの使用

一部の銀行では、銀行にログインするときに、その都度セキュアソフトトークンサービスによって生成されるOTP(One-Time Password: ワンタイムパスワード)を使用できるようにするために、顧客にセキュアソフトトークンサービスに登録することを要求しています。Trusteer Rapportは、パートナーにセキュアソフトトークンサービスを提供しています。このサービスは、ユーザーのコンピューターに潜んでいるマルウェアが、OTPを生成したり、盗んだりすることを防止する追加の保護機能を備えています。ご利用の銀行がTrusteer Rapportのセキュアソフトトークンサービスに加入している場合は、以下の説明に従ってサービスを有効にし、必要に応じてOTPを生成して、生成されたOTPを管理してください。

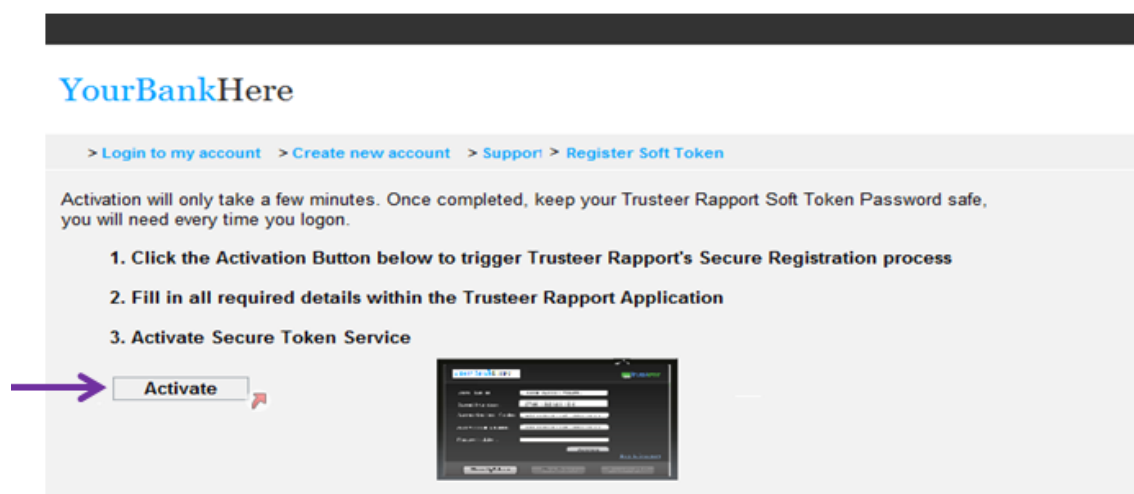
セキュアソフトトークンの有効化

ワンタイムパスワードの生成を可能にするには、セキュアソフトトークンサービスを有効にする必要があります。

➔ Trusteer Rapportのセキュアソフトトークンの有効化方法

1. 銀行から、シリアル番号、認証コード、およびアクティベーションコードを受け取ったら、銀行Webサイトのログインページをブラウズします。

2. 銀行からの指示に従って、アクティベーションプロセスを開始します。
たとえば、以下のような画面で[登録]ボタンをクリックする必要がある場合があります。



[トークンの登録]画面が表示されます。

The screenshot shows a "Token Activation" screen with a green header and a "RAPPORT" logo. The main content area is purple and contains the following text: "Step 1 out of 3", "Please select a User name and password for this token. You will be able to identify this token based on the user name selected here and will be asked to provide the password in order to generate a one time password." Below this is a "Help & Support" link with a dropdown arrow. There are three input fields labeled "User Name:", "Password:", and "Retype Password:". At the bottom, there are "Next" and "Cancel" buttons.

- 表示されたフィールドに、ご希望のユーザー名およびパスワードを入力し、もう一度パスワードを入力します。ここで入力するユーザー名およびパスワードは、ワンタイムパスワードを生成する必要が生じたときに、その都度ソフトトークンサービスにログインするために使用するものです。
- [次へ]をクリックします。以下の画面が表示されます。

Token Activation RAPPORT

Step 2 out of 3

To complete secure activation, complete all fields below using the data you have received from your bank.

[Help & Support](#) ▼

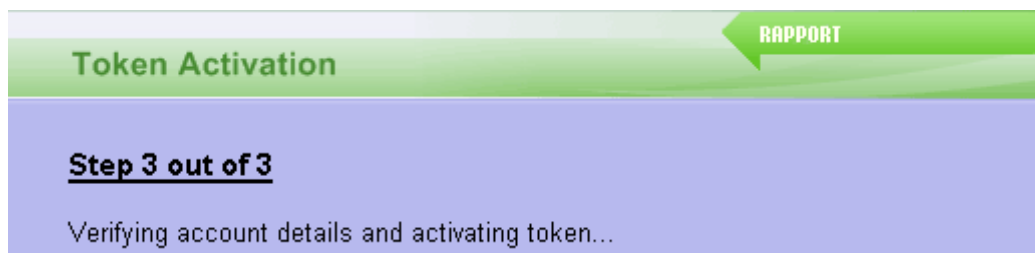
Serial Number:

Authorization Code:

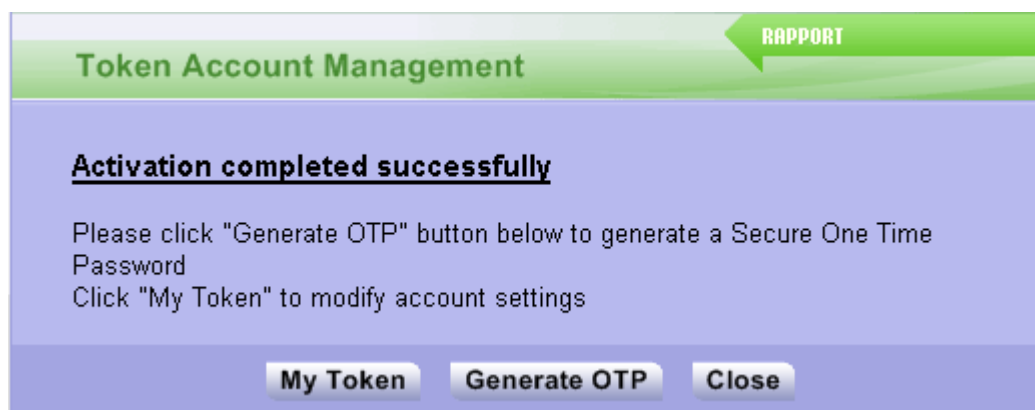
Activation Code:

- 表示されたフィールドに、銀行から提供されたアクティベーション情報の詳細を入力します。
- [登録]をクリックします。以下の画面が表示されます。

注: [登録]をクリックする前に、このフィールドに入力した情報が銀行から送信された情報と正確に一致していることを確認してください。情報が間違っていると、ワンタイムパスワードの生成がブロックされてしまう可能性があります。この場合、銀行のカスタマーサポートに連絡する必要があります。



入力した詳細の検証が終了すると、以下の画面が表示されます。

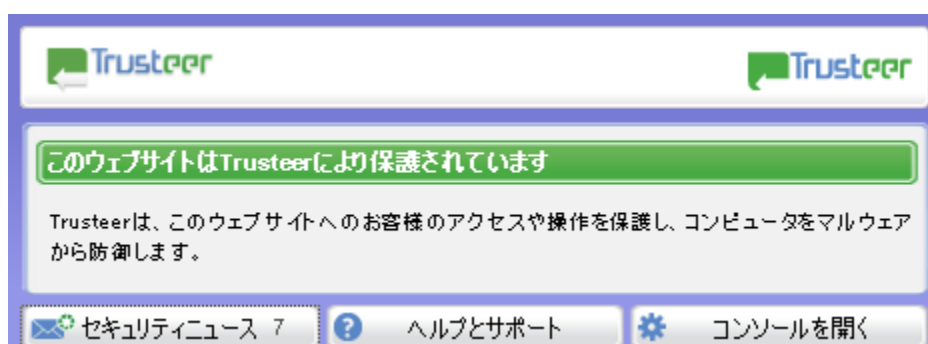


[OTPを生成する]ボタンを使用して、ただちにワンタイムパスワードを生成できます。

OTPの生成

→ OTPの生成方法

1. ご利用の銀行のWebサイトのログインページをブラウザします。
2. トークンを生成するように要求された場合は、プロンプトダイアログの指示に従います。
3. トークンを生成するように要求されない場合は、Trusteer Rapportアイコンをクリックします。[トークンを生成する]ボタンが表示されたRapportステータスインジケータが表示されます。



4. [トークンを生成する]をクリックします。[トークンの生成]画面が表示されます。


5. [ユーザー名]ドロップダウンリストから、ログインする口座のソフトウェアトークンサービスを有効にしたときに作成したユーザー名を選択します ([「セキュアソフトウェアトークンの有効化」](#) (83ページ)を参照)。
6. [パスワード]フィールドに、ユーザー名フィールドで選択したトークンアカウントに対するパスワードを入力します。
7. [生成する]をクリックします。新しいワンタイムパスワードが生成され、[ワンタイムパスワード]フィールドに表示されます。パスワードをクリップボードにコピーします。
8. [閉じる]をクリックします。[トークンの生成]画面が閉じます。新しいワンタイムパスワードが、自動的に銀行のログインフォームにコピーされます。
9. 銀行のログイン画面で、ワンタイムパスワードが[パスワード]フィールドに自動的にコピーされていることを確認します。コピーされていない場合は、フィールドにパスワードを貼り付け、これを使用して口座にログインします。

OTPアカウントの管理

ご利用の銀行のWebサイトでTrusteer RapportのOTPを有効にすると、OTPアカウントが作成されます。Trusteer Rapportのセキュアソフトウェアトークンサービスに加入している銀行の口座を複数お持ちの場合は、複数のOTPアカウントを持つことができます。 [「OTPアカウントの名称変更」](#) (89ページ)および [「OTPアカウントの削除」](#) (90ページ)で説明されているように、Rapportコンソールを使用してOTPアカウントの名前を変更したり、削除したりできます。

OTPアカウントの名称変更

→ OTPアカウントの名称変更方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。




3. [OTPアカウント]領域で、[OTPアカウントを管理する]をクリックします。
[トークンアカウントの管理]タブが表示されます。
4. [ユーザー名]フィールドで、名前を変更するアカウントのユーザー名を選択します。
5. [新しいユーザー名]フィールドに、新しいユーザー名を入力します。
6. [名前を変更する]をクリックします。確認メッセージが表示されます。

7. [はい]をクリックします。アカウントの名前が変更されます。

OTPアカウントの削除

関連する銀行口座を閉鎖した場合、または銀行がトークンのアクティベーション詳細を再発行した場合は、既存のOTPアカウントを削除することをお奨めします。

➔ OTPアカウントの削除方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [OTPアカウント]領域で、[OPアカウントを管理する]をクリックします。
[トークンアカウントの管理]タブが表示されます。

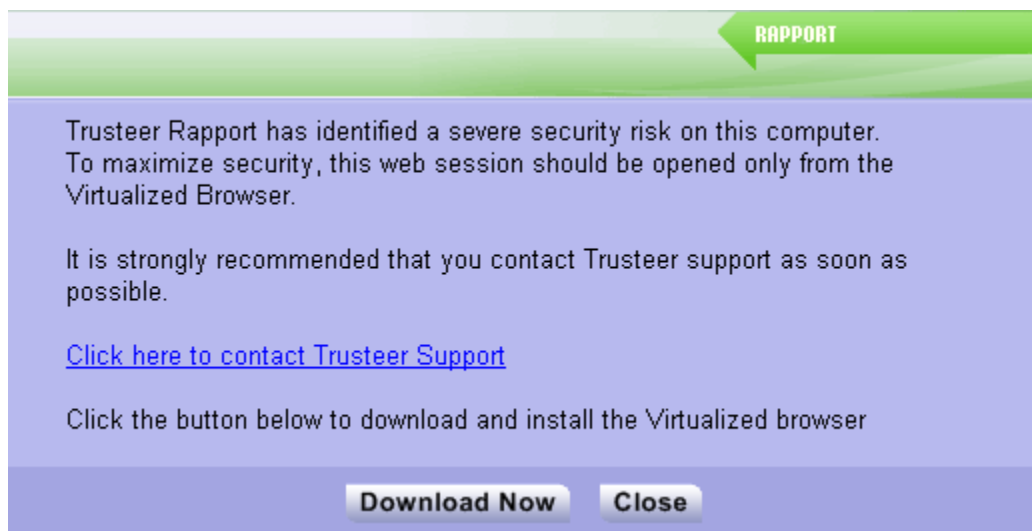
4. [ユーザー名]フィールドで、削除するアカウントのユーザー名を選択します。
5. [削除する]をクリックします。確認メッセージが表示されます。
6. [はい]をクリックします。アカウントが削除されます。

10.アラートおよび警告への応答

Trusteer Rapportでは、ユーザーの応答を必要とするアラートや警告が表示される場合があります。Trusteer Rapportのダイアログボックスが表示されたら、内容をよく読み、適切な応答を選択してください。要求されたアクションを実行することが、セキュリティを確保するうえで非常に重要な場合があります。以下に、表示されるダイアログボックスの例と、応答方法を示します。

仮想化ブラウザの強制ダウンロードアラートに対する応答

以下に、仮想化ブラウザの強制ダウンロードアラートの例を示します。



このアラートは、保護されたWebサイトをブラウズしたときに表示される場合があります。このアラートは、Trusteer Rapportにより、ユーザーのコンピュータ上でセキュリティリスクが検知されたため、そのサイトを通常のブラウザで表示することが阻止されたことを示しています。サイトを表示するには、Trusteer Rapportの仮想化ブラウザをダウンロードしてインストールする必要があります。Trusteer Rapportの仮想化ブラウザは、追加の保護レイヤーを提供する、隔離されたブラウジング環境です。

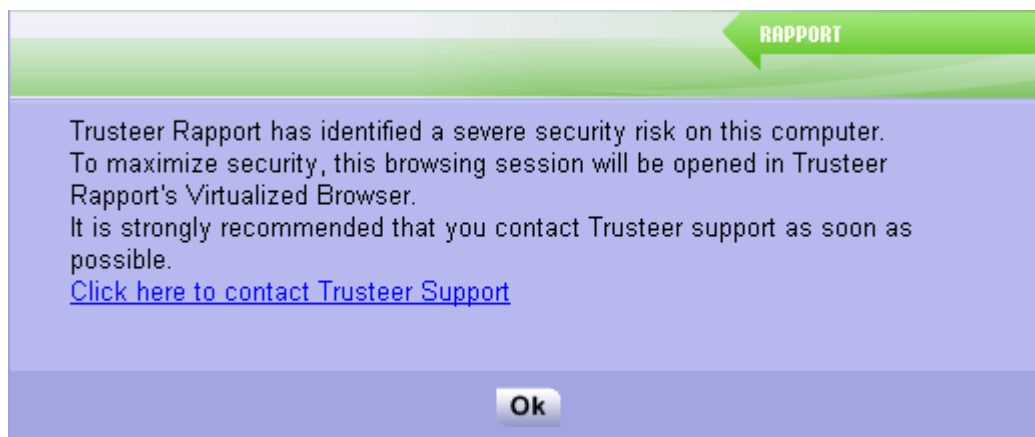
このアラートが表示されたら、以下のいずれかのオプションを選択します。

- **[ダウンロード]**をクリックします。Trusteer Rapportの仮想化ブラウザのインストールファイルがダウンロードされます。このファイルをダウンロードして実行した後は、当該のサイトを再度ブラウザすると、仮想化ブラウザで安全に表示できます。また、Trusteerサポート([「ユーザー問題レポートの送信」](#) (234ページ))を参照)に、このアラートが表示されたことをご連絡いただくことをお奨めします。弊社から、ご使用のコンピューターに潜んでいるセキュリティリスクへの対抗措置についてご案内します。
- **[Trusteerのサポートに連絡するために、ここをクリックしてください]**をクリックします。Rapportコンソールで**[問題をレポートする]**フォームが開きます。このフォームを使用して、当該のアラートが表示されたことをTrusteerにご連絡ください。弊社から、ご使用のコンピューターに潜んでいるセキュリティリスクへの対抗措置についてご案内します。問題のレポートの詳細については、[「ユーザー問題レポートの送信」](#) (234ページ)を参照してください。
- **[閉じる]**をクリックします。アラートとWebサイトが閉じます。

Trusteer Rapportの仮想化ブラウザをダウンロードおよびインストールする方法の詳細については、[「Trusteer Rapportの仮想化ブラウザの使用」](#) (79ページ)を参照してください。

仮想化ブラウザの強制アラートに対する応答

以下に、仮想化ブラウザの強制アラートの例を示します。



このアラートは、保護されたWebサイトをブラウズしたときに表示される場合があります。このアラートは、Trusteer Rapportにより、ユーザーのコンピュータ上でセキュリティリスクが検知されたため、そのサイトを通常のブラウザで表示することが阻止されたことを示しています。このサイトを閲覧するには、Trusteer Rapportの仮想化ブラウザで表示する必要があります。仮想化ブラウザは、以前このサイトを開いた際に、ユーザーのコンピュータにインストールされています。Trusteer Rapportの仮想化ブラウザは、追加の保護レイヤーを提供する、隔離されたブラウジング環境です。

このアラートが表示されたら、以下のいずれかのオプションを選択します。

- **[Trusteerのサポートに連絡するために、ここをクリックしてください]** をクリックします。Rapportコンソールで**[問題をレポートする]**フォームが開きます。このフォームを使用して、当該のアラートが表示されたことをTrusteerにご連絡ください。弊社から、ご使用のコンピュータに潜んでいるセキュリティリスクへの対抗措置についてご案内します。問題のレポートの詳細については、[「ユーザー問題レポートの送信」](#) (234ページ)を参照してください。
- **[OK]** をクリックします。当該のサイトがTrusteer Rapportの仮想化ブラウザで開きます。

仮想化ブラウザのオプションダウンロードアラートに対する 応答

以下に、仮想化ブラウザのオプションダウンロードアラートの例を示します。



このアラートは、Trusteer Rapportの仮想化ブラウザをサポートしているWebサイトをブラウズしたときに表示されます。Trusteer Rapportの仮想化ブラウザは、ご使用のコンピューターに潜んでいるマルウェアに対抗するための追加の保護レイヤーを提供する、隔離されたブラウジング環境です。

このアラートが表示されたら、以下のいずれかのオプションを選択します。

- **[ダウンロード]**をクリックします。Trusteer Rapportの仮想化ブラウザのインストールファイルがダウンロードされます。このファイルをダウンロードして実行した後は、当該のサイトを再度ブラウズすると、仮想化ブラウザで安全に表示できます。
- **[このサイトでは再通知しない]**をクリックします。仮想化ブラウザをダウンロードせずにアラートが閉じます。以降このサイトを再度表示しても、このアラートは表示されません。当該のサイトは通常のブラウザで開きます。
- **[この警告メッセージを再出力しない]**をクリックします。仮想化ブラウザをダウンロードせずにアラートが閉じます。以降、仮想化ブラウザをサポートしているサイトを表示しても、このアラートは表示されません。当該のサイトは通常のブラウザで開きます。

- **[閉じる]**をクリックします。アラートが閉じ、当該のサイトが通常のブラウザで開きます。


Trusteer Rapportの仮想化ブラウザをダウンロードおよびインストールする方法の詳細については、[「Trusteer Rapportの仮想化ブラウザの使用」](#) (79ページ)を参照してください。

誤って[この警告メッセージを再出力しない]をクリックしてしまいました。それでも仮想化ブラウザでサイトを開くことはできますか。

[「仮想化ブラウザのオプションダウンロードアラートに対する応答」](#) (95ページ)または[「仮想化ブラウザのオプションアラートに対する応答」](#) (101ページ)の操作で[この警告メッセージを再出力しない]をクリックすると、セキュリティポリシーが変更され、以降仮想化ブラウザをサポートしているサイトをブラウズしても、アラートは表示されなくなります。このポリシーは、以下の手順でリセットできます。

➔ 仮想化ブラウザアラートポリシーのリセット方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。




6. **[Trusteer Rapportの仮想化ブラウザを対応サイトで使用することを推奨する]**というコントロールが表示されるまで、下にスクロールします。
 このコントロールの右側にあるドロップダウンメニューから、**[常に]**を選択してポリシーをデフォルト設定にリセットします。
7. **[保存する]**をクリックします。ポリシーの変更が保存されます。これ以降、仮想化ブラウザをサポートしているサイトをブラウズすると、Trusteer Rapportによりそのサイトを仮想化ブラウザで開くかどうか尋ねられます。

[このサイトでは再通知しない]をクリックしましたが、仮想化ブラウザで開くことが必要になりました。どのように操作すれば良いでしょうか。

[「仮想化ブラウザのオプションダウンロードアラートに対する応答」](#) (95ページ)の操作で[この警告メッセージを再出力しない]をクリックすると、セキュリティポリシーが変更され、以降このサイトをブラウザしても、仮想化ブラウザに関するアラートは表示されなくなります。このポリシーはリセットできます。

➔ サイトの仮想化ブラウザポリシーの変更方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。
5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。ここには、すべてのセキュリティコントロールが表示されています。



6. [Trusteer Rapportの仮想化ブラウザを対応サイトで使用することを推奨する]というコントロールが表示されるまで、下にスクロールします。
[以下のサイトに対して、仮想化ブラウザのアラートを表示しないことを選択しました。]の下で、対象Webサイトの[サイトを削除する]ボタンをクリックします。

7. **[保存する]**をクリックします。ポリシーの変更が保存されます。以降、このサイトをブラウズしたときに、Trusteer Rapportにより仮想化ブラウザのアラートが表示されます。

仮想化ブラウザのオプションアラートに対する応答

以下に、仮想化ブラウザのオプションアラートの例を示します。



このアラートは、仮想化ブラウザがすでにインストールされているコンピュータで、Trusteer Rapportの仮想化ブラウザをサポートしているサイトをブラウズしたときに表示されます。このアラートでは、このサイトを仮想化ブラウザで開くかどうかを尋ねるオプションが表示されます。

このアラートが表示されたら、以下のいずれかのオプションを選択します。

- **[はい]**をクリックして、Trusteer Rapportの仮想化ブラウザでサイトを開きます。**[このサイトを登録する]**チェックボックスをオンにしておくと、次回以降このサイトは自動的に仮想化ブラウザで開きます。
- Trusteer Rapportの仮想化ブラウザの詳細を確認するには、**[仮想化ブラウザとはなんですか?]**をクリックします。
- **[いいえ]**をクリックして、通常のブラウザでサイトを開きます。**[このサイトを登録する]**チェックボックスをオンにしておくと、次回以降アラートは表示されず、このサイトは自動的に通常のブラウザで開きます。


- [\[この警告メッセージを再出力しない\]](#)をクリックして、仮想化ブラウザをサポートしているサイトが、デフォルトでこのアラートを表示せずに通常のブラウザで開くように、Trusteer Rapportのポリシーを変更します。当該のサイトは通常のブラウザで開きます。

誤って[\[この警告メッセージを再出力しない\]](#)をクリックしてしまいました。それでも仮想化ブラウザでサイトを開くことはできますか。

[「仮想化ブラウザのオプションダウンロードアラートに対する応答」](#) (95ページ)または[「仮想化ブラウザのオプションアラートに対する応答」](#) (101ページ)の操作で[\[この警告メッセージを再出力しない\]](#)をクリックすると、セキュリティポリシーが変更され、以降仮想化ブラウザをサポートしているサイトをブラウズしても、アラートは表示されなくなります。このポリシーは、以下の手順でリセットできます。

➔ 仮想化ブラウザアラートポリシーのリセット方法

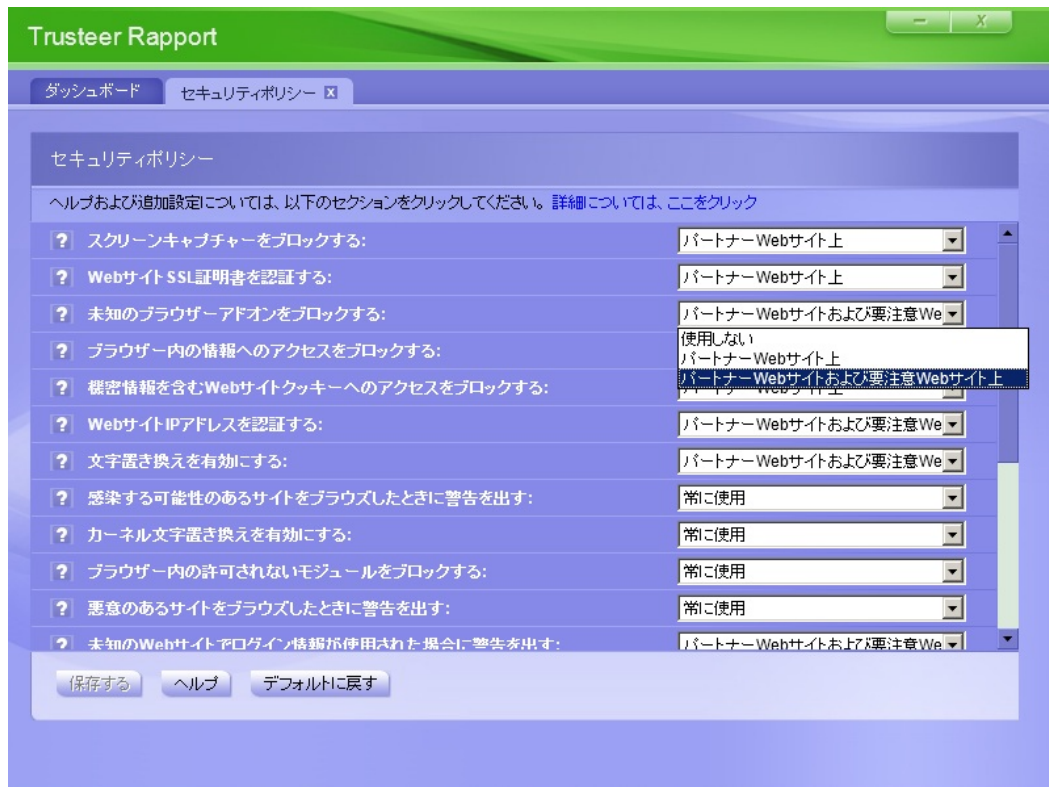
1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここには、すべてのセキュリティコントロールが表示されています。




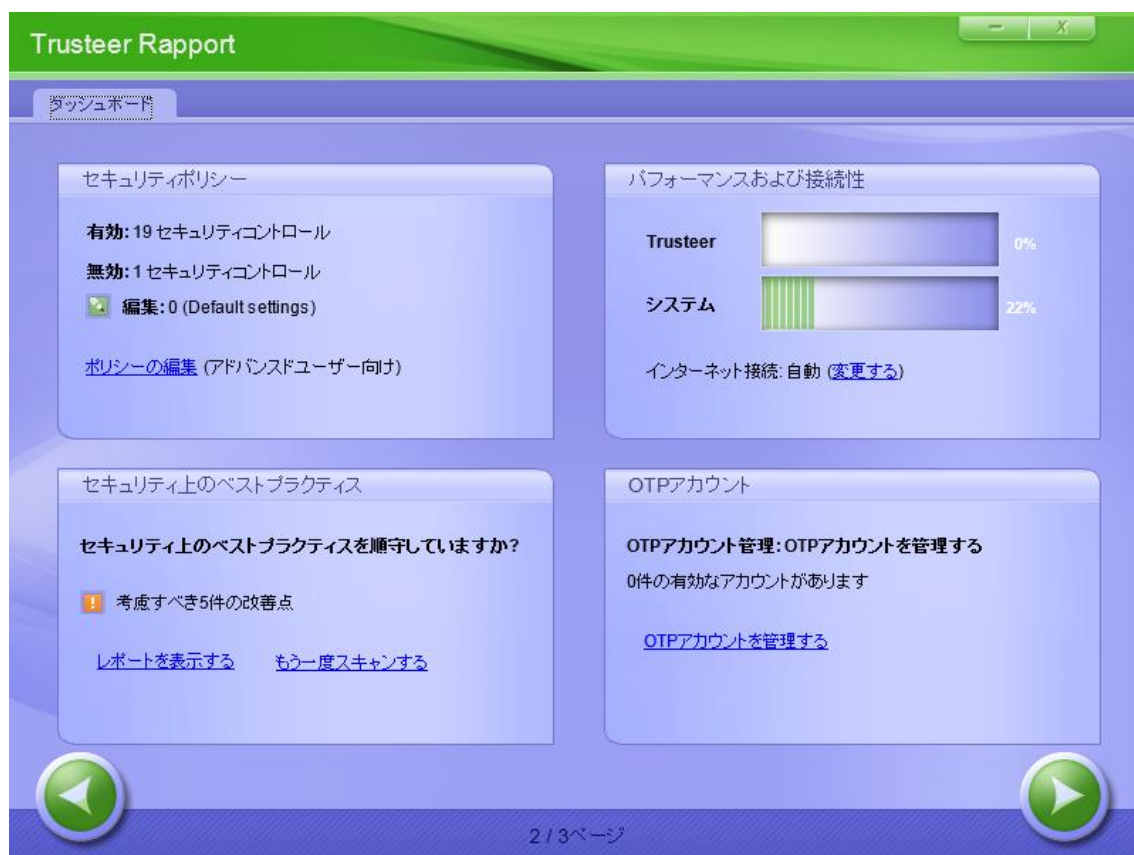
6. **[Trusteer Rapportの仮想化ブラウザを対応サイトで使用することを推奨する]**というコントロールが表示されるまで、下にスクロールします。
このコントロールの右側にあるドロップダウンメニューから、**[常に]**を選択してポリシーをデフォルト設定にリセットします。
7. **[保存する]**をクリックします。ポリシーの変更が保存されます。これ以降、仮想化ブラウザをサポートしているサイトをブラウズすると、Trusteer Rapportによりそのサイトを仮想化ブラウザで開くかどうか尋ねられます。

[はい]をクリックし、**[このサイトを登録する]**チェックボックスをオンにしましたが、このサイトを通常のブラウザで開くことが必要になりました。どのように操作すれば良いでしょうか。

セキュリティポリシーを変更して、このサイトを通常のブラウザで開くように、オプションを復元することができます。

➔ サイトの仮想化ブラウザポリシーの変更方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

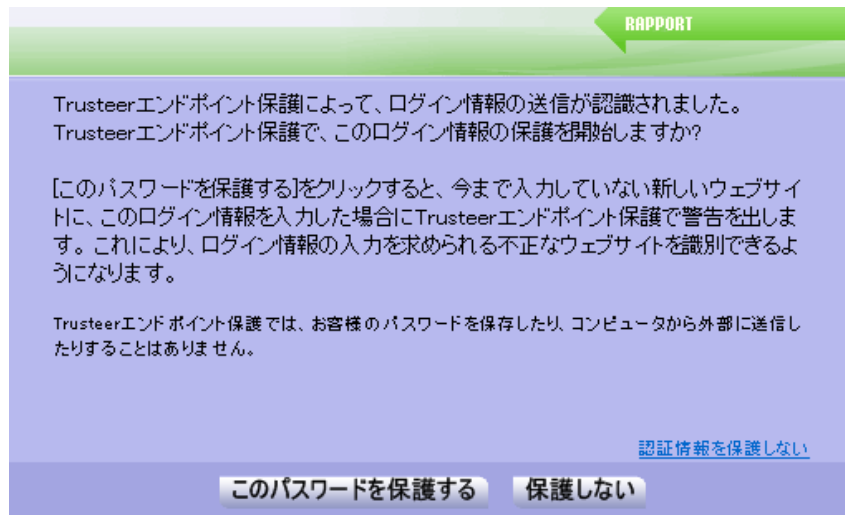
5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。



6. [Trusteer Rapportの仮想化ブラウザーを対応サイトで使用することを推奨する]というコントロールが表示されるまで、下にスクロールします。
 [仮想化ブラウザーで次のサイトを開く]の下で、対象Webサイトの[サイトを削除する]ボタンをクリックします。
7. [保存する]をクリックします。ポリシーの変更が保存されます。

パスワード保護の提示に対する応答

以下に、パスワード保護の提示の例を示します。



パスワード保護の提示は、保護された各Webサイトで、1回表示されます。これは、保護されたWebサイトに対してパスワードを入力していることをTrusteer Rapportが検知したときに、初回のみ表示されます。たとえば、ご利用の銀行のWebサイトからTrusteer Rapportをダウンロードし、その後初めてそのWebサイトにログインした場合、このダイアログボックスが表示されます。その他、手動でWebサイトに保護を追加し、その後初めてそのWebサイトにログインした場合も、このダイアログボックスが表示されます。

Trusteer Rapportが認識していないWebサイトに、保護されているパスワードを入力した場合は、Trusteer Rapportにより、異なるWebサイトにパスワードを使用しようとしていることを知らせる警告が表示されます。この警告により、パスワードが不正なWebサイトに送信されないよう、防ぐことができます。これは、[フィッシング攻撃](#)³からユーザーを守るうえで役立ちます。

³ フィッシング攻撃は、銀行のWebサイトなどの信頼済みWebサイトに見せかけた偽のWebサイトにユーザーを誘導し、オンラインのログイン情報を送信させようとするものです。犯罪者は、その情報を利用してユーザーのオンライン口座にアクセスし、ユーザーの銀行口座から送金を行うなどの詐欺行為を行います。

この提示が表示されたら、以下のいずれかのオプションを選択します。

- **[保護する]**をクリックします。この操作を実行した後は、Trusteer Rapportにより、このWebサイトでパスワードが保護されます。パスワードが変更されたら、Trusteer Rapportはユーザーに尋ねることなく、自動的に新しいパスワードを保護します。
- **[保護しない]**をクリックします。このオプションを選択すると、Trusteer Rapportはこのサイト上ではいかなるパスワードも保護せず、これ以降ユーザーがこのサイトを開いても、パスワード保護の提示は表示されません。
- **[パスワードを保護しない]**をクリックします。このオプションを選択すると、すべてのWebサイトに対して、Trusteer Rapportのアンチフィッシング保護が無効になります。これをクリックすると、以降Trusteer Rapportからパスワード送信に関して警告が表示されることはなくなります。また、すべてのWebサイトで、パスワード保護の提示が表示されなくなります。

間違ったパスワードを保護してしまいました。どうすれば良いでしょうか。

正しいパスワードを入力し直せば問題ありません。Trusteer Rapportにより、そのパスワードが保護されます。


パスワードを間違っって入力し、保護することを選択してしまいました。どうすれば良いでしょうか。

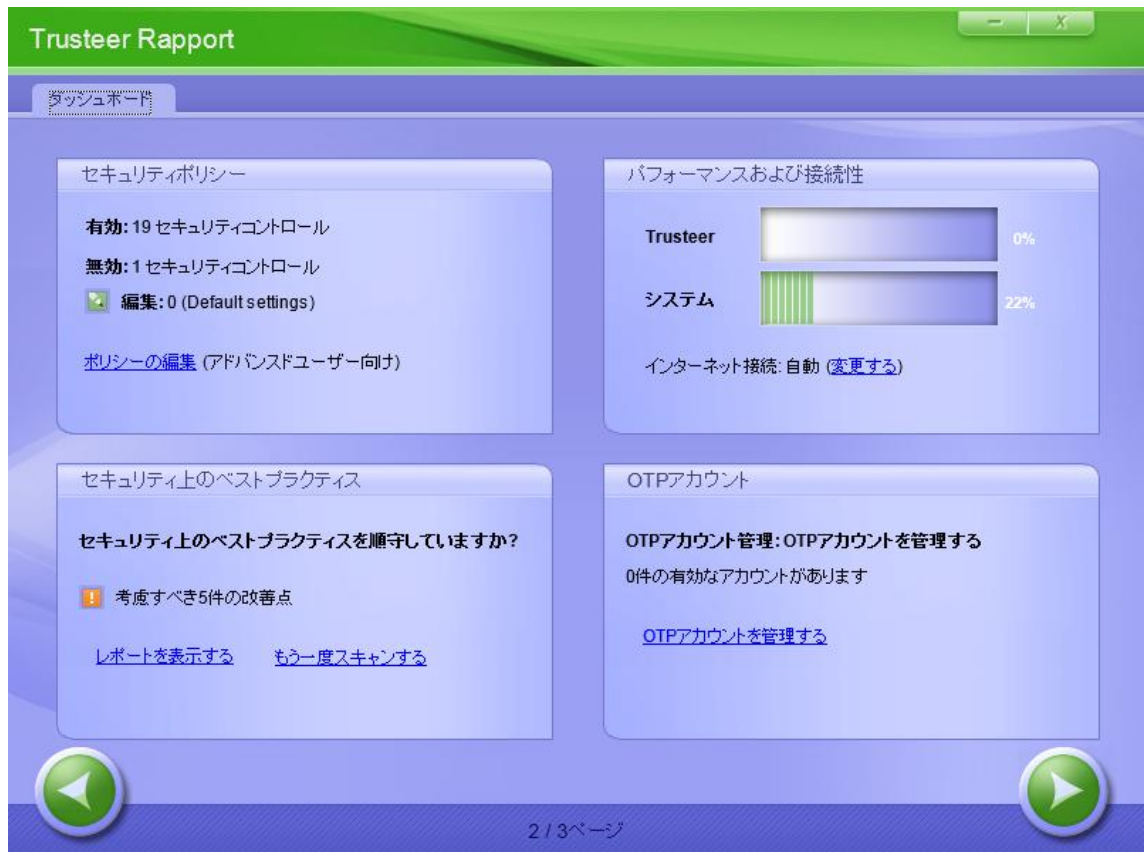
パスワードを入力し直せば問題ありません。Trusteer Rapportにより、正しいパスワードが保護されます。

[パスワードを保護しない]を選択しましたが、パスワード保護が必要になりました。どのように操作すれば良いでしょうか。

[パスワードを保護しない]を選択した場合、Trusteer Rapportのセキュリティポリシーに、ポリシー定義が設定されています。このポリシーは変更できます。

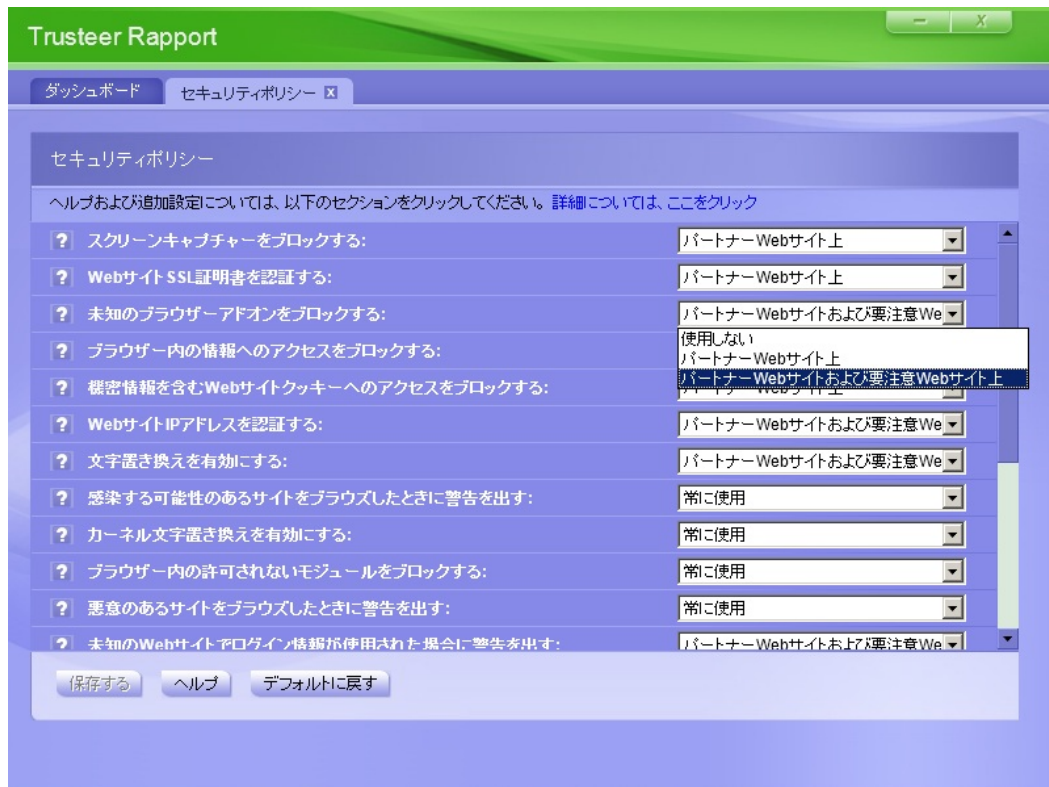
➔ パスワード保護ポリシーの変更方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。ここには、すべてのセキュリティコントロールが表示されています。




6. [未知のWebサイトでログイン情報が使用された場合に警告を出す]というコントロールを見つけます。このコントロールの右側にあるドロップダウンメニューで、[パートナーおよびお客様の機密情報のWebサイト上]を選択してデフォルト設定にリセットするか、パートナーのWebサイト上だけでパスワード保護の提示を希望する場合は、[パートナーのWebサイト上]を選択します。

7. [保存する]をクリックします。ポリシーの変更が保存されます。

[保護しない]を選択しましたが、パスワード保護が必要になりました。どのように操作すれば良いのでしょうか。

特定のWebサイトに対するパスワード保護の定義を変更することができます。

➔ パスワード保護を無効にした特定のWebサイトで、パスワード保護を有効化する方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。

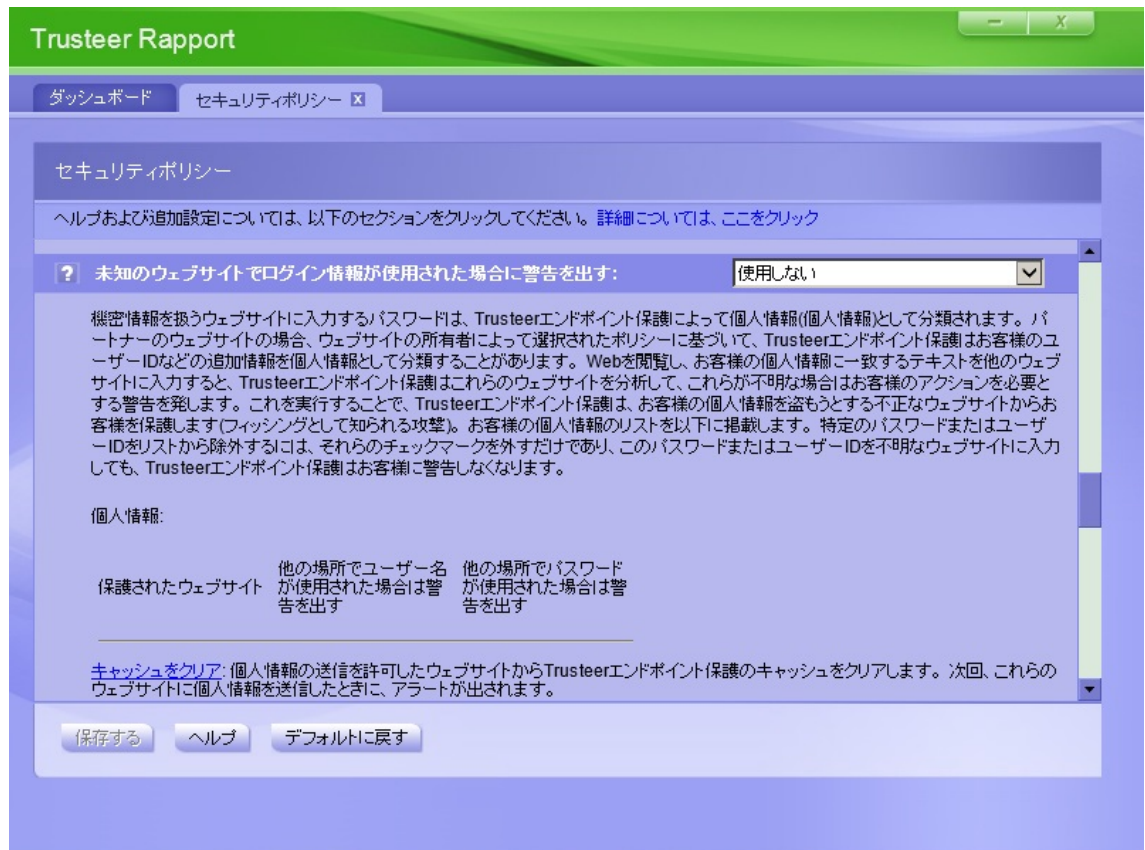


3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。



6. [未知のWebサイトでログイン情報が使用された場合に警告を出す]をクリックします。各Webサイトのユーザー名およびパスワードに対する保護ポリシーが表示されます。




7. パスワード保護を有効にするWebサイトに対する[他の場所でパスワードが使用された場合は警告を出す]チェックボックスをオンにします。これで、Trusteer Rapportにより当該のWebサイトのパスワードが保護されます。
8. [保存する]をクリックします。ポリシーの変更が保存されます。

使用していないパスワードのアラートが表示されます。これを停止するにはどうすれば良いでしょうか。

パートナーWebサイトとの取り決めによっては、パスワードが変更された後も、パスワードの保護が継続される場合も多くあります。安全なパスワードであれば、その他の目的には使用されないため、この点が問題になることはまれです。それでも古いパスワードについてTrusteer Rapportによる保護を停止する必要がある場合は、PII (Personally Identifiable Information: 個人情報) キャッシュをクリアして、パスワード保護メカニズムをリセットしてください。この操作により、Trusteer Rapportによる古いパスワードの保護は停止しますが、次に保護された各Webサイトを開いたときに、新たにパスワード保護が提示されます。

➔ PIIキャッシュをクリアする方法

1. [「Rapportコンソールのオープン」](#) (72ページ) を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。
5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。ここには、すべてのセキュリティコントロールが表示されています。
6. セキュリティコントロールのリストを下にスクロールして、[未知のWebサイトでログイン情報が使用された場合に警告を出す]を見つけます。

7. [未知のWebサイトでログイン情報が使用された場合に警告を出す]をクリックします。各Webサイトのユーザー名およびパスワードに対する保護ポリシーが表示されます。



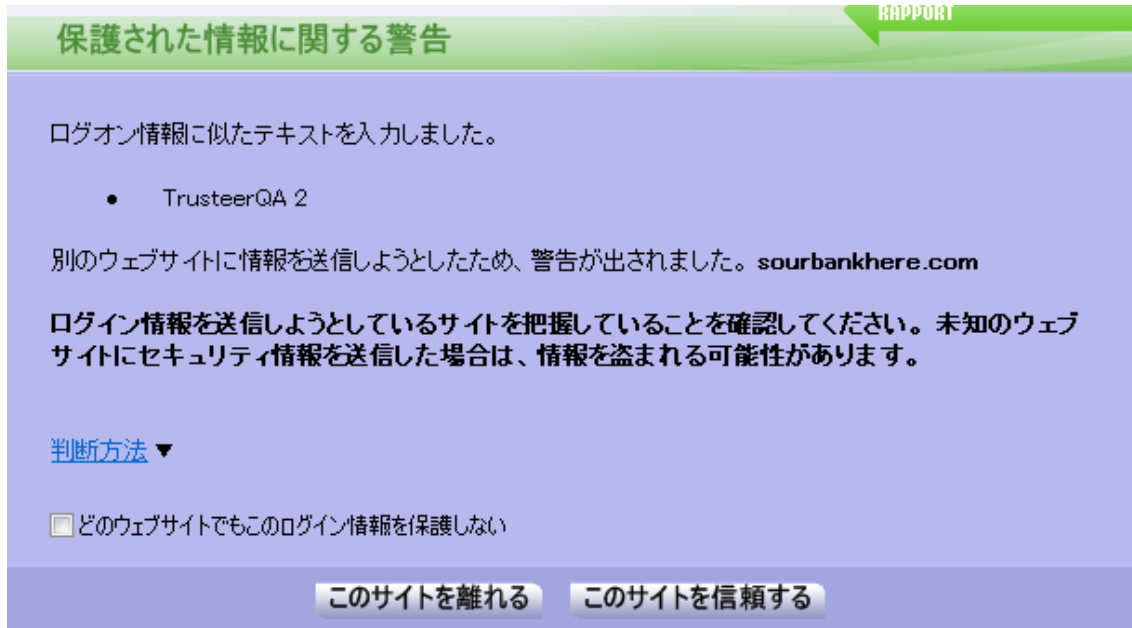
- 8.
9. [キャッシュをクリアする]をクリックします。すべてのパスワード保護がクリアされ、すべてのパスワード保護ポリシーがリセットされます。これにより、次回以降各Webサイトを表示した際に、Trusteer Rapportによりパスワード保護の提示が表示されます。

パスワードを保護したサイトとば別のサイトで、その保護されたパスワードを入力しましたが、警告は表示されませんでした。なぜでしょうか。

正規のサイトの中には、Trusteer Rapportにより、正規であることが確認済みである場合があります。そのようなサイトでパスワードを入力しても詐欺行為に結びつくことは無いため、Trusteer Rapportはこのようなサイトでは警告を生成しません。

保護情報の警告に対する応答

以下に、保護情報の警告の例を示します。



保護された情報に関する警告

ログオン情報に似たテキストを入力しました。

- TrusteerQA 2

別のウェブサイトに情報を送信しようとしたため、警告が出されました。 **sourbankhere.com**

ログイン情報を送信しようとしているサイトを把握していることを確認してください。未知のウェブサイトにセキュリティ情報を送信した場合は、情報を盗まれる可能性があります。

[判断方法](#) ▼

どのウェブサイトでもこのログイン情報を保護しない

[このサイトを離れる](#) [このサイトを信頼する](#)

保護情報の警告は、Trusteer Rapportが認識していないWebサイトに、保護されているユーザー名またはパスワードに一致するテキストを入力した場合に表示されます。このメッセージボックスの目的は、現在ユーザーが情報を送信しようとしているWebサイトが、ユーザーの機密情報を盗もうとしている不正なWebサイトでは無いことを確認することにあります。これは、フィッシング攻撃として知られています。

上記の例では、Trusteer Rapportは、www.example-phishing.comというWebサイト(実在のサイトではありません)が、google.comに見せかけた偽のサイトではなく、ユーザーにgoogle.comの認証情報を入力させようとしているものではないことを確認しようとしています。

この警告が表示されたら、以下のいずれかのオプションを選択します。

- このサイトが別のWebサイトの認証情報を要求しているのではないことが分かっており、このWebサイトにログイン情報を送信して問題ない場合は、**[このサイトを信頼する]**をクリックします。このボタンをクリックした後は、当該の保護されたユーザー名およびパスワードをこのWebサイトに入力しても、警告は表示されません。入力したテキストがログイン情報ではない場合、または複数のWebサイトでそのログイン情報を使用しており、当該のテキストを入力するたびにアラートが表示されることを避けたい場合は、**[ログイン情報を保護しない]**をクリックしても構いません。

注: セキュリティを実践するうえで、パスワードは一意で予想が難しいフレーズであること、かつ同じパスワードを複数のWebサイトで使用しないことを推奨します。この実践方法に従った場合、**[ログイン情報を保護しない]**チェックボックスをオンにする必要はほとんどありません。

- このWebサイトにログイン情報を送信しない場合は、**[このサイトへ移動しない]**をクリックします。リダイレクト先のサイトを選択するように促すダイアログボックスが表示されます。

なぜ保護情報の警告が多数表示されるのでしょうか。

複数の異なるサイト上で、同じでテキストをパスワードとして日常的に入力している場合、パスワードが保護されているサイト以外のWebサイトでそのテキストを入力するたびに、保護情報の警告が表示されます。これによるストレスを回避したい場合は、このようなパスワードを保護しないでください。機密情報をやりとりするWebサイトに、このようなパスワードを使用している場合は、より安全なパスワードに変更することを強くお奨めします。安全なパスワードとは、使用するWebサイトに対して一意であり、予想することが難しい文字の羅列で構成されています。通常は、文字、数字、記号の組み合わせで構成されています。

Trusteer Rapportで保護されていないWebサイトに保護されたパスワードを入力しましたが、アラートは表示されませんでした。なぜでしょうか。

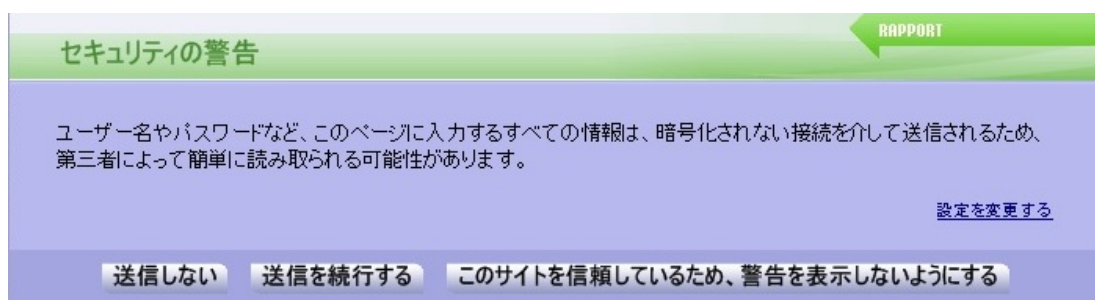
Trusteer Rapportは、複数の手法を使用して、一部のWebサイトを正規のものであると認識しています。Trusteer Rapportがアラートを表示すべき場合に表示しなかったと思われる場合は、[「サポートについて」](#) (210ページ)を参照して、サポートにお問い合わせください。

保護されたパスワードを入力していないのに保護情報の警告が表示されました。なぜでしょうか。

一部の保護されたWebサイトでは、ユーザーがTrusteer Rapportをインストールした後に、そのWebサイトに入力したすべてのパスワードが保護されます。これには、古いパスワードや、そのサイトに誤って入力したテキストも含まれます。これが、この警告が表示される理由として考えられます。

安全でない送信の警告に対する応答

以下に、安全でない送信の警告の例を示します。



この警告は、データを安全に送信しないWebサイトにユーザーがパスワードを入力した場合に表示されます。この警告の目的は、リスクの高いサイトへの機密情報の送信を防止するものです。リスクの高いサイトには、犯罪者が簡単に情報をインターセプトできる正規Webサイトも含まれます。

このメッセージが表示されたら、以下のいずれかを実行します。


- **[送信しない]**をクリックします。ブラウザーが、安全でないサイトに送信するリスクについて説明したTrusteerのWebサイトにリダイレクトされます。
- **[送信する]**をクリックして、警告にかかわらず送信を続行します。
- **[信頼済みサイトなので、再警告を出力しない]**をクリックして、警告にかかわらず送信を続行し、今後このサイトを信頼することをTrusteer Rapportに知らせます。このボタンをクリックすると、このサイトが信頼済みサイトのリストに追加され、今後Trusteer Rapportによる警告は表示されなくなります。信頼済みサイトのリストからこのサイトを削除する場合は、[「安全でない送信警告用の信頼済みサイトのクリア」](#) (222 ページ)を参照してください。
- **[設定の変更]**をクリックしてTrusteer Rapportのセキュリティポリシー画面を開き、このような警告を表示するかどうかを制御する**[安全ではないサイトにセキュリティデータを送信する場合に警告する]**ポリシーを変更します。

[信頼済みサイトなので、再警告を出力しない]をクリックしましたが、信頼済みサイトのリストからサイトを削除することはできますか。

はい、できます。

➔ 信頼済みサイトのリストからサイトを削除する方法

1. [「Rapportコンソールのオープン」](#) (72 ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。

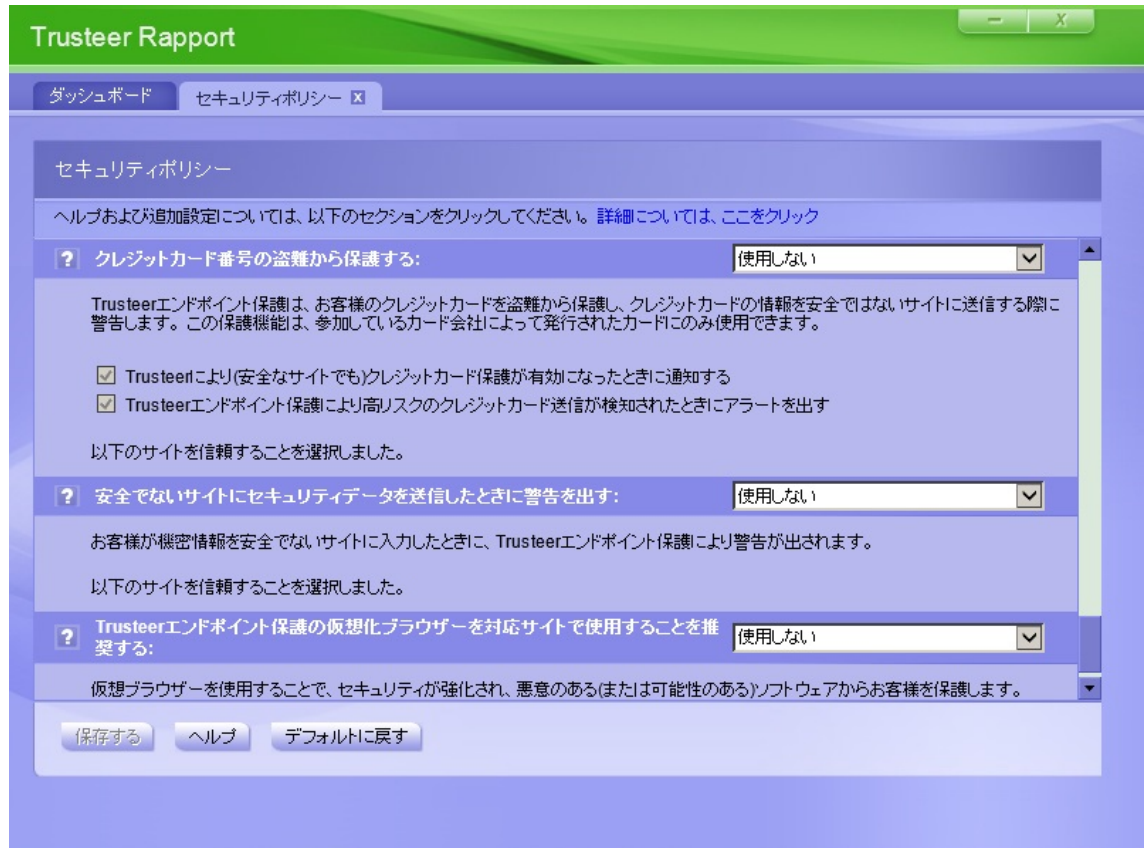


3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。



6. [安全ではないサイトにセキュリティデータを送信する場合に警告する]というポリシーコントロールをクリックします。[以下のサイトを信頼することを選択しました。]という文言と、信頼することを選択したサイトのリストが表示されます。



7. ホワイトリストに追加したサイトを見つけ、サイト名の横に表示されている[このサイトをクリアする]ボタンをクリックします。
8. [保存する]をクリックします。ポリシーの変更が保存されます。

フィッシングサイトの警告に対する応答

以下に、フィッシングサイトの警告の例を示します。

Trusteerエンドポイント保護 不正防御 **RAPPORT**

www.sourbankhere.comのウェブページにアクセスしようとしています。このウェブサイトは既知のフィッシングサイトであり、セキュリティを確保するため、Trusteerによってブロックされました。

フィッシングサイトは、正規のサイトを装って、お客様の機密情報を盗み取るように設計されています。

このページに情報を入力すると、なりすまし犯罪や金銭的な損失などの被害に遭う可能性があります。

[この警告を無視する](#)

このサイトを離れる **このページがブロックされた理由**

この警告は、ユーザーが開こうとしたWebサイトが、(通常フィッシングサイトと呼ばれる)偽のWebサイトであることがTrusteer Rapportにより確認されたため、Webサイトの閲覧がブロックされた場合に表示されます。Trusteer Rapportは、フィッシングWebサイトを正確に検知する総合的な機能を備えています。疑わしいWebサイトにアクセスしたときに表示されるこの警告は、お客様がフィッシング関連の詐欺の被害者になることを防止するために提供されています。Webサイトへのリンクをクリックした後にこの警告が表示された場合は、リンクは不正なものである可能性が非常に高く、リスクは甚大です。

この警告が表示されたら、以下のいずれかのオプションを選択します。

- **[このサイトへ移動しない]**をクリックします。ブラウザーが前回アクセスしたサイトにリダイレクトされます。
- **[ページがブロックされた理由]**をクリックします。この警告が表示された理由を説明するWebページが開きます。

- **[警告メッセージを無視する]**をクリックします。レポートされたリスクにかかわらず、Webサイトがロードされます。これを選択すると、口座にログインするための機密の認証情報を盗むために犯罪者が作成したと確認されているWebサイトにアクセスすることになります。一部のフィッシングWebサイトでは、送信ボタンを押さなくても、入力するだけでデータが犯罪者に送信されます。犯罪者は、そのデータを利用してなりすまし犯罪や詐欺を行います。**このオプションを選択しないことを強くお奨めします。**


正規のWebサイトがフィッシングサイトと認識されている場合

正規のWebサイトがフィッシングサイトとして認識されていると思われる場合は、サイトおよび表示された警告のスクリーンショットを、support@trusteer.comまでお送りください。

詐欺防止警告を無効化する場合

➔ **詐欺防止警告の無効化方法**

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここでは、すべてのセキュリティコントロールが表示されています。



6. **[悪意のあるサイトをブラウズしたときに警告を出す]**というコントロールを**[しない]**に設定します。
7. **[保存する]**をクリックします。ポリシーの変更が保存されます。

感染したWebページの警告に対する応答

以下に、感染したWebページの警告の例を示します。

Trusteerエンドポイント保護 不正防御 RAPPORT

アクセスしようとしているehuth1.trusteer.comのウェブサイトは安全ではないため、お客様のコンピュータが悪意のあるソフトウェアに感染する可能性があります。

サイト所有者の知らないうちに、正規のウェブサイトに悪意のあるコンテンツが組み込まれることがあります。これらのサイトを閲覧したコンピュータは、ユーザーが知らないうちに悪意のあるソフトウェアに感染して、後でお客様のオンラインバンキングアカウントから金銭を盗むなどの違法行為を犯すこともあります。このサイトを引き続き閲覧した場合、危険なマルウェアに感染する可能性があります。

[無視してエラーをレポートする](#)

このサイトを離れる **このページがブロックされた理由**

このダイアログボックスは、ユーザーが開こうとしたページが、ユーザーのコンピュータにマルウェアを感染させる可能性がある場合に表示されます。Trusteer Rapportは、ユーザーがオンライン詐欺の被害者になることを防ぐために、この保護を提供しています。

このダイアログボックスが表示されたら、以下のいずれかのオプションを選択します。

- **[このサイトへ移動しない]**をクリックします。ブラウザーが、ご使用のホームページにリダイレクトされます。
- **[ページがブロックされた理由]**をクリックします。この警告が表示された理由を説明するWebページ

(<https://www.trusteer.com/support/trusteer-fraud-prevention-infected-webpage>)が開きます。

- [エラーをレポートして無視する]をクリックします。レポートされたりリスクにかかわらず、Webサイトがロードされます。また、匿名のレポートがTrusteerのサーバーに送信されます。これを選択すると、レポートされているリスクにかかわらずサイトの表示を続行することになり、ユーザーのコンピューターがマルウェアに感染するおそれがあります。

クレジットカード情報送信検知の警告に対する応答

以下に、クレジットカード情報送信検知の警告の例を示します。

警告 RAPPORT

安全でないまたは高リスクのウェブサイトへのクレジットカード情報の入力を検知しました。安全でないサイトではカード情報を入力しないことをお勧めします。

[このサイトを常に信頼する](#) [カードの保護を停止する](#)

このサイトを離れる **このウェブサイトを信頼するため、無視する**

この警告は、ローカルドライブまたは安全でないWebサイト上に存在するWebページに、保護されたクレジットカード番号を入力するたびに表示されます。このメッセージボックスは、フィッシングWebサイトまたは安全でない正規のWebサイトへの、クレジットカード番号の送信を回避することを目的としています。

この警告が表示されたら、以下のいずれかを実行します。

- このWebサイトにカード情報を送信しない場合は、[このサイトへ移動しない]をクリックします。ブラウザーはこのWebサイトから離れ、代わりにホームページがロードされます。

- このWebサイトにカード情報を送信して問題ない場合は、**[信頼済みサイトなので、無視する]**をクリックします。ダイアログボックスは閉じますが、Trusteer Rapportはキーロガーによるクレジットカード情報のキャプチャーのブロックを継続します。クレジットカードの発行元は、この送信についての通知を受信します。信頼済みサイトからこのサイトを削除する場合は、[「クレジットカード情報送信用の信頼済みサイトのクリア」](#) (219ページ)を参照してください。

注: この警告を無視することを選択すると、クレジットカード情報は、既知の悪意のあるWebサイトか、またはクレジットカード情報を暗号化していないため、第三者がこの情報を閲覧できる状態にあるサイトに送信することになります。

- **[常に信頼するサイト]**をクリックします。Trusteer Rapportはこのサイトを信頼し、今後このサイトにクレジットカード情報を入力しても、この警告が再度表示されることは無くなります。Trusteer Rapportは、キーロガーによるクレジットカード情報のキャプチャーのブロックを継続します。
- **[クレジットカード保護機能を停止]**をクリックします。クレジットカードの保護機能が無効になります。この機能を再度有効にする場合は、**[クレジットカードの番号を盗難から保護する]**ポリシーを**[しない]**から**[常に]**に変更します。セキュリティポリシーの変更方法については、[「セキュリティコントロールの変更」](#) (189ページ)を参照してください。

注: クレジットカード保護は、登録しているカード会社のカードのみで有効です。

クレジットカード保護のメッセージに対する応答

以下に、クレジットカード保護のメッセージの例を示します。



このメッセージは、ユーザーがクレジットカード番号をWebページに送信しようとしていること、およびキーロギングマルウェアによるクレジットカード番号のキャプチャーを防止するために、ページ上でキーストロークを暗号化していることを、Trusteer Rapportが検知したことを通知するものです。このメッセージは、Trusteer Rapportにより保護されたサイトまたはVisa、MasterCard、Amexなどのクレジットカードに関連するキーワードが含まれるその他の安全な(https)サイトにユーザーがクレジットカード番号を入力したときに表示されます。

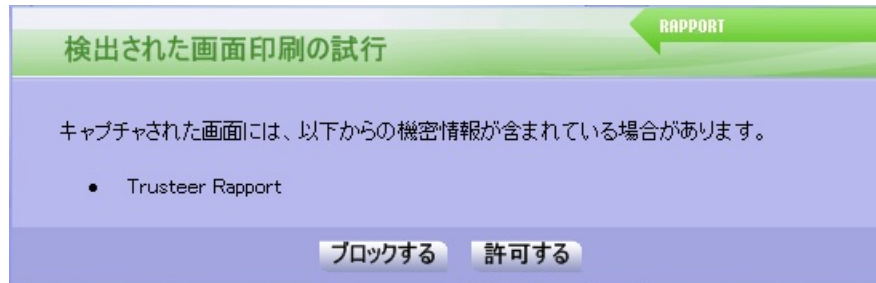
このメッセージが表示されても、何もする必要はありません。任意で[OK]をクリックし、メッセージを閉じることもできます。何もしなくても、しばらく経過するとメッセージは自動的に閉じます。

Trusteer Rapportがアンチキーロギングをアクティブにしたときに通知を受け取らないようにするには、[メッセージを再表示しない]をクリックします。これらの通知を再度有効にする場合は、セキュリティポリシーを開き、[クレジットカードの番号を盗難から保護する]ポリシーの下にある[クレジットカード保護機能が有効になった時に通知]チェックボックスをオンにします。セキュリティポリシーにアクセスし、変更する方法については、[「セキュリティコントロールの変更」](#) (189ページ)を参照してください。

注: クレジットカード保護は、登録しているカード会社のカードのみで有効です。

[プリントスクリーン検知]アラートに対する応答

以下に、[プリントスクリーン検知]アラートの例を示します。



このダイアログボックスは、ブラウザでパートナーのWebサイトを表示しているときに、ご使用のコンピューターでPrint Screenコマンドボタンが押された場合に表示されます。このダイアログボックスでは、スクリーンキャプチャーメカニズムをブロックするか、許可するかを選択できます。

キーボードのPrint Screenコマンドボタンは、画面をキャプチャーするために合法的に使用されます。ただし、マルウェアによりこのボタンにより作動するメカニズムと同じメカニズムが作動し、不正使用の目的で機密情報が詐取されるおそれがあります。

注: このアラートはスクリーンキャプチャーのブロック機能の一部であり、パートナーのWebサイト上ではデフォルトで有効になっています。Trusteer Rapportのキャプチャーブロック機能の詳細については、[「セキュリティポリシーコントロールについて」\(194ページ\)](#)を参照してください。

この警告が表示されたら、以下のいずれかのオプションを選択します。

- **[許可]**をクリックします。Print Screenコマンドボタンによる画面のキャプチャーが許可されます。意図的にPrint Screenコマンドボタンを押して画面をキャプチャーしようとしている場合は、このオプションを選択します。

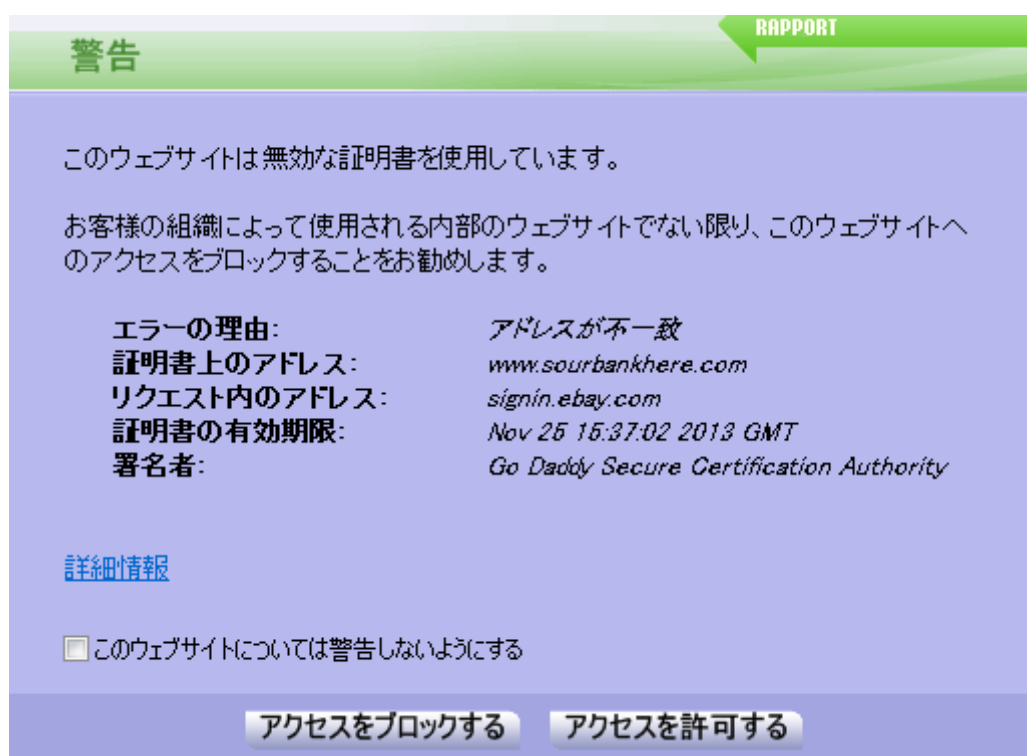
- [ブロック]をクリックします。Print Screenコマンドボタンによる画面のキャプチャーがブロックされます。意図的にキーボードのPrint Screenコマンドボタンを押していない場合は、このオプションを選択します。

機密情報のサイトのキャプチャーを試行していないがダイアログが表示される場合

すべてのブラウザーウィンドウを最小化するか閉じてから、再試行してください。

ブラウザー保護アラートに対する応答

以下に、[Rapport Browser Protection]アラートの例を示します。




このダイアログボックスは、ブラウザーのアドオン(ツールバー、拡張機能など)により、現在Trusteer Rapportでは監視されていない方法を使用して、保護されたWebサイトに属する情報へのアクセスが試行された場合に表示されます。このダイアログボックスが表示されたら、以下のいずれかのオプションを選択します。

- **[常に許可]**をクリックします。このオプションを選択すると、Trusteer Rapportは、どのWebサイト上でもこのアドオンの動作を許可します。ブラウザでのアドオンの機能を認識している場合、このアドオンを使用している場合、およびこのアドオンのソースを信頼している場合は、このオプションを選択します。
- **[常にブロック]**をクリックします。このオプションを選択すると、Trusteer Rapportは、どのWebサイト上でもこのアドオンの動作を阻止し、Trusteerに匿名でブロックされたアドオンについてのセキュリティレポートを送信します。このレポートは、弊社のセキュリティ専門スタッフが解析します。このレポートを送信していただくことにより、このアドオンが悪意のあるものであると判明した場合は、Trusteerはグローバルかつ恒久的にこのアドオンをブロックすることができるようになります。

一度ブロックしたアドオンのブロック解除/許可したアドオンのブロックについて

➔ **ブロックまたは許可したアドオンの変更方法**

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

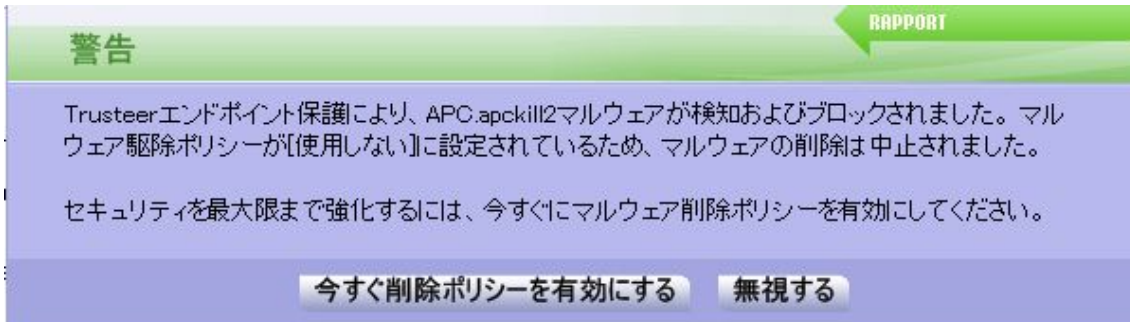
5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここには、すべてのセキュリティコントロールが表示されています。



6. **[未知のブラウザーアドオンをブロックする]**ポリシー名をクリックします。ポリシー名の下に、許可またはブロックしたすべてのアドオンのリストが表示されます。
7. 必要に応じて、各アドオンのステータスを切り替えます。
8. **[保存する]**をクリックします。変更内容が保存されます。

マルウェア駆除の有効化アラートに対する応答

以下に、マルウェア駆除の有効化アラートの例を示します。



このアラートは、マルウェアの駆除ポリシーが無効になっているときに、Trusteer Rapportがマルウェアを検知してブロックした場合に表示されます。このアラートの目的は、ユーザーがマルウェアの駆除ポリシーを有効にして、Trusteer Rapportによるマルウェアの駆除を可能にすることにあります。マルウェアの駆除はデフォルトで有効になっていますが、Rapportのセキュリティポリシーで無効になっている場合があります ([「Trusteer Rapportのセキュリティポリシーの変更」](#) (187ページ)を参照)。

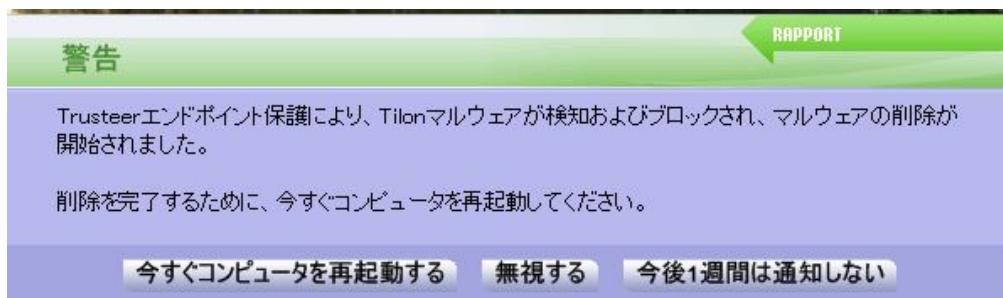
このアラートが表示されたら、以下のいずれかを実行します。

- **[今すぐ削除ポリシーを有効にする]**をクリックします。マルウェアの駆除ポリシーが有効になり、Trusteer Rapportによりブロックされたマルウェアの駆除が開始されます。別のダイアログボックスが表示され、再起動を促される場合があります。この場合、**[今すぐコンピュータを再起動する]**をクリックする前に、開いているファイルおよびアプリケーションを保存して閉じることができます。再起動により、マルウェアの駆除が完了します。

- [無視する]をクリックします。次回Trusteer Rapportがマルウェアを検知したときに、アラートが再度表示されます。マルウェアはブロックされますが、コンピューター上には残ります。ブロックされたマルウェアがコンピューターに残っていると、今後Trusteer Rapportが停止されたり削除されたりした場合、またはRapportがサポートしていないブラウザを使用した場合に、マルウェアがアクティブになる可能性があるため、危険です。

マルウェア駆除の開始アラートに対する応答

以下に、マルウェア駆除の開始アラートの例を示します。



Trusteer Rapportがマルウェアを検知し、ブロックして、コンピューターからの駆除を開始したときに、このようなアラートが表示されます。マルウェアの駆除を完了するために、Trusteer Rapportからコンピューターの再起動を求められます。

このアラートが表示されたら、以下のいずれかを実行します。

- **[今すぐコンピュータを再起動する]**をクリックします。ただちにコンピュータが再起動されます。再起動により、マルウェアの駆除が完了します。再起動後、Trusteer Rapportの保護されたWebサイト上で口座にログインしたときに、Trusteer Rapportのアイコンが緑色になっていることを確認してください。再起動後は、マルウェア駆除の開始アラートダイアログボックスが再度表示されることはありません。コンピュータを再起動した後でもこのアラートが表示される場合は、[「ユーザー問題レポートの送信」](#) (234ページ)を参照して、Rapportコンソールからユーザー問題レポートを送信してください。
- **[無視する]**をクリックします。マルウェアの駆除は、次回コンピュータを再起動したときに完了します。コンピュータを再起動するまでは、オンラインでの機密情報の使用は避けてください。このマルウェアの駆除について、Trusteer Rapportにより再度アラートが表示されることはありません。
- **[今後1週間は通知しない]**をクリックします。マルウェアが残っている場合、1週間後に再度アラートが表示されます。その間に再起動していれば、マルウェアの駆除は完了し、アラートが再度表示されることは無くなります。

アンインストール中のマルウェア感染アラートに対する応答

以下に、アンインストール中のマルウェア感染アラートの例を示します。



このダイアログボックスは、アンインストールプロセスを開始した場合に、Trusteer RapportがPC上で悪意のあるソフトウェアを検知すると表示されます。このダイアログボックスでは、PCにマルウェアが存在していることを知ったうえで、Trusteer Rapportのアンインストールを取りやめて元に戻すことができます。マルウェアの中には、オペレーティングシステムや個人情報に危険にさらすことなく駆除することが不可能なものもあります。Trusteer Rapportでは、このようなマルウェアは駆除せず、ブロックして無効化しています。

注: 現在、Trusteer Rapportではブロックされたマルウェアの名前は表示されません。弊社では、この点を変更するように取り組んでいます。ブロックされたマルウェアの詳細については、[「ユーザー問題レポートの送信」](#) (234ページ)を参照して、Rapportコンソールからユーザー問題レポートを送信してください。

このダイアログボックスが表示されたら、以下のいずれかのオプションを選択します。

- **[続行する]**をクリックします。アンインストール処理が再開します。
- **[中止する]**をクリックします。アンインストール処理が中止されます。

弊社では、処理を中止し、Trusteer Rapportをアンインストールしないことを強くお奨めします。Trusteer Rapportが他のプログラムに干渉している場合、または何らかの問題の原因になっていると思われる場合は、[「Trusteer Rapportの停止」](#) (207 ページ) を参照してTrusteer Rapportを停止し、<http://www.trusteer.com/support/submit-ticket>のフォームを使用して、サポートリクエストを弊社までお送りください。この問題が解決するまで、オンラインバンキングや会社へのWebアクセスなどの、機密情報を扱うアクティビティを行わないことをお奨めします。

無効な証明書の警告への応答

以下に、無効な証明書の警告の例を示します。

警告
RAPPORT

このウェブサイトは無効な証明書を使用しています。

お客様の組織によって使用される内部のウェブサイトでない限り、このウェブサイトへのアクセスをブロックすることをお勧めします。

エラーの理由:	アドレスが不一致
証明書上のアドレス:	<i>www.sourbankhere.com</i>
リクエスト内のアドレス:	<i>signin.ebay.com</i>
証明書の有効期限:	<i>Nov 25 15:37:02 2013 GMT</i>
署名者:	<i>Go Daddy Secure Certification Authority</i>

[詳細情報](#)

このウェブサイトについては警告しないようにする

アクセスをブロックする
アクセスを許可する

このダイアログボックスは、保護されたWebサイトをブラウズしたときに、Trusteer Rapportにより、そのWebサイトの**証明書⁴**が無効であることが検知された場合に表示されます。無効な証明書とは、失効している、間違いがある、または未知の発行者によって署名されている、などの証明書です。このダイアログボックスの目的は、不正なWebサイトに情報を送信することを阻止することにあります。

注: コンピューターの日付または時刻が正確に設定されていない場合、有効な証明書を持つWebサイトでもこの警告が表示される場合があります。この警告が頻繁に表示される場合は、ご使用のコンピューターの日付および時刻を確認してください。

無効な証明書の警告では、以下の情報が表示されます。

表示フィールド 説明

[エラーの理由]

Trusteer Rapportがこの警告を発した理由。

以下のいずれかの値が表示されます。

- **[アドレスに矛盾があります]:** アクセスしようとしたアドレスと、証明書のアドレスが一致しません。有効な証明書に記載されたアドレスは、実際のアドレスと一致している必要があります。2つのアドレスを確認してください。証明書に記載されたアドレスが疑わしい、またはアクセスしようとしているWebサイトと無関係である場合は、アクセスをブロックすることを選択してください。
- **[不明な電子証明書の署名者]:** Trusteerは、証明書に署名した認証局を確認していません。未知の認証局は、有効な証明書の発行元として信頼しないでください。銀行および金融機関は、必ず既知の署名者により発行された証明書を使用します。
- **[期限切れ証明書]:** 証明書の有効期限が過ぎているため、有効ではなくなっています。失効した証明書を使用しているWebサイトは、セキュリティ基準が低いと言えます。銀行および金融機関では、失効している証明書を使用することは絶対にありません。コンピューターのクロックをチェックして、コンピューターの日付が正しいことを確認してください。コンピューターのクロックが現在の日付よりも進んでいる場合は、このメッセージが誤って表示されている可能性があります。
- **[無効な証明書]:** 証明書のフォーマットが正しくありません。

⁴ SSL証明書は、暗号化されたデジタル証明書で、WebサイトのIDを検証し、Webサイトに機密の個人データを送信するための暗号化された接続を確立します。ブラウザーのアドレスバーまたはブラウザーの下部にSSLの南京錠が表示された場合は、SSLプロトコルを使用して、ブラウザーとWebサイト間の安全な接続が確立されていることを意味します。ただし、これは証明書が有効であることを通知するものではありません。

表示フィールド	説明
[発行元]	このWebサイトから提示された証明書に記載されているアドレス。各証明書は、特定のWebアドレスに対して発行されています。各Webサイトで提示される証明書には、そのWebサイト自体のアドレスが表示されている必要があります。
[接続先]	ブラウザが誘導されたWebアドレス。これは、アクセスしようとしたアドレスです。
[有効期限]	各証明書には、有効期限が設けられています。失効した証明書を使用しているWebサイトは、セキュリティ基準が低いと言えます。
[署名者]	この証明書を発行した認証局。未知の認証局から発行された証明書は、信頼しないでください。


このダイアログボックスが表示されたら、以下のいずれかのオプションを選択します。

- **[接続をブロック]**をクリックします。サイトへのアクセスがブロックされます。このWebサイトが金融機関またはショッピングのサイトであり、ユーザーが機密情報を送信するものである場合は、このオプションを選択します。
- **[接続を許可]**をクリックします。サイトへのアクセスが許可されます。このWebサイトがローカルネットワーク上(イントラネット)にある場合、または機密情報を扱うものではない場合は、このオプションを選択できます。アクセスを許可する場合、操作は慎重に行い、機密情報は送信しないでください。**[このサイトで再警告を出力しない]**チェックボックスは、今後このWebサイトについてTrusteer Rapportのアラートを表示しないようにする場合のみ、オンにしてください。

この機能を無効化する方法

Trusteer Rapportコンソールを使用して、SSL証明書の検証を停止することができます。この操作により、Trusteer RapportによるWebサイトの証明書の妥当性チェックが停止し、この警告は表示されなくなります。

➔ SSL証明書検証の無効化方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

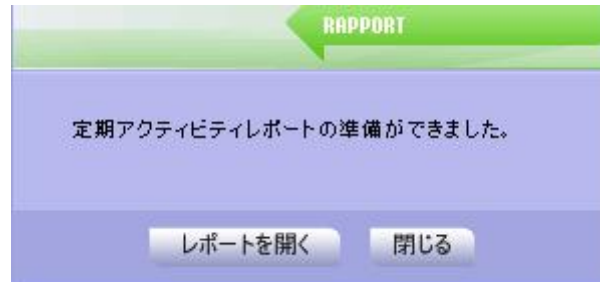
5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここでは、すべてのセキュリティコントロールが表示されています。



6. **[WebサイトのSSL証明書を検証する]**というコントロールを見つけます。
7. このコントロールの右側にあるドロップダウンリストで、**[しない]**を選択します。
8. **[保存する]**をクリックします。以上で、SSL証明書の検証が無効になります。

アクティビティレポートの通知に対する応答

以下に、週次アクティビティレポートの通知の例を示します。



このダイアログボックスは、Rapportコンソールでアクティビティレポートを生成([「アクティビティレポートの設定」](#)(168ページ)を参照)するオプションを選択している場合に、1週間に1度表示されます。

この通知が表示されたら、以下のいずれかを実行します。

- **[レポートを開く]**をクリックします。Rapportコンソールが開き、週次アクティビティレポートが表示されます。
- **[閉じる]**をクリックします。アラートが閉じ、アクティビティレポートは表示されません。ただし、アクティビティレポートは随時確認できます([「アクティビティレポートの表示」](#)(166ページ)を参照)。

1週間以上経過しましたが、週次アクティビティレポートが表示されません。なぜでしょうか。

週次アクティビティレポートは、過去1週間以内に1つ以上のイベントが発生した場合のみ表示されます。ログに記録されたイベントが存在しない可能性もあります。

Trusteer Rapportのアップグレードのプロンプトに対する応答

以下に、Trusteer Rapportのアップグレードのプロンプトの例を示します。



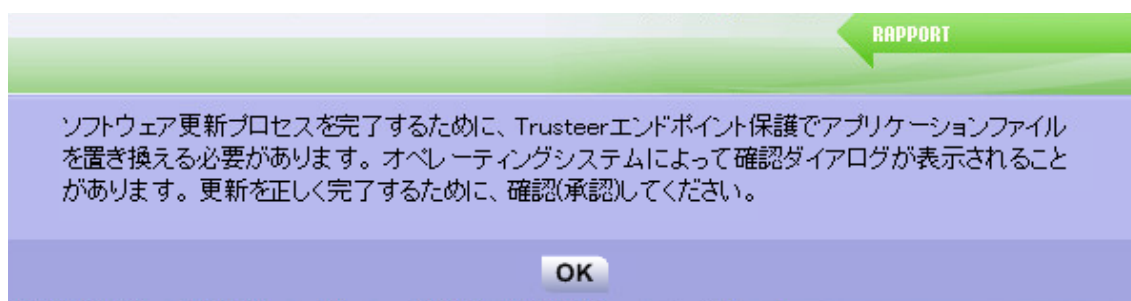
このダイアログボックスは、手動で保護するWebサイトを追加しようとしたときに、サイトを追加することによって、ライセンスで許可されている、保護できるWebサイトの最大数を超過してしまう場合に表示されます。このダイアログボックスから、ライセンスをアップグレードして、保護するWebサイトの数を無制限にすることができます。

このダイアログボックスが表示されたら、以下のいずれかを実行します。

- **[今すぐRapportをアップグレード]**をクリックします。TrusteerのWebサイトが開き、ライセンスをアップグレードできます。アップグレードは無償です。
- **[キャンセル]**をクリックします。試行していたWebサイト保護の操作がキャンセルされ、ライセンスはアップグレードされません。
- 既存のWebサイトの保護を解除してから、新たに別のWebサイトの保護を追加してください。詳細については、[「保護されたWebサイトの管理」](#) (181ページ)を参照してください。

コード更新の管理メッセージに対する応答

ご使用のコンピューターでユーザーアカウント制御(Windows 7およびWindows Vistaの保護機能)が有効になっている場合、Trusteer Rapportの自動更新時にこのメッセージが表示される場合があります。

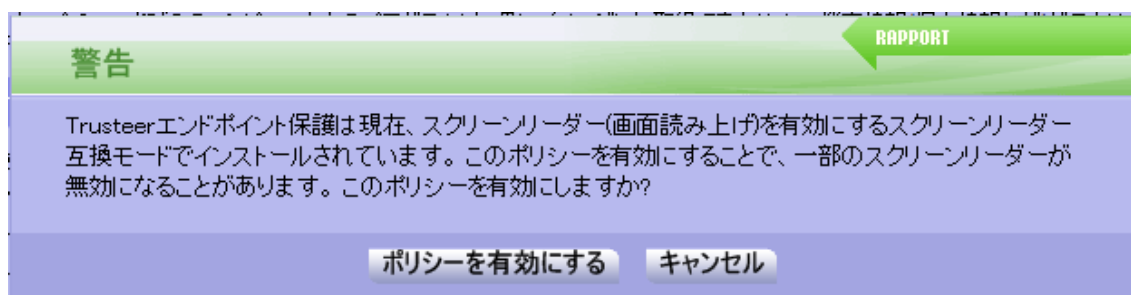


このメッセージが表示されたら、**[OK]**をクリックしてください。ユーザーアカウント制御のダイアログボックスが表示され、Trusteer Rapportの更新プロセス続行の許可を求められます。ユーザーアカウント制御メッセージが表示されたら、**[続行する]**をクリックしてアップデートを完了します。

注: コード更新の確認メッセージが頻繁に表示される場合は、Trusteerのサポート (<http://www.trusteer.com/support/submit-ticket>) にお問い合わせください。

画面読み上げ互換モードの警告に対する応答

以下に、画面読み上げ互換モードの警告の例を示します。



Trusteer Rapportが画面読み上げ互換モードでインストールされている場合、以下のセキュリティポリシーの1つを有効にしようとすると、このような警告が表示されます(セキュリティポリシーの有効化および無効化の詳細については、[「セキュリティコントロールの変更」](#)(189ページ)を参照)。

- [スクリーンキャプチャーをブロックする]
- [ブラウザー内の情報へのアクセスをブロックする]

Trusteer Rapportが画面読み上げ互換モードでインストールされている場合、これらのポリシーは、デフォルトで無効になります。これらのポリシーのいずれかを有効にすると、画面読み上げソフトウェアの機能に干渉し、WebページおよびTrusteer Rapportのメニューおよびダイアログの読み上げができなくなるおそれがあります。

この警告が表示されたら、以下のいずれかを実行します。

- [ポリシーを有効にする]をクリックします。ポリシーを有効化すること間違いはなく、コンピューターの画面読み上げ機能がTrusteer Rapportにアクセスできなくなっても問題ない場合は、このオプションを選択します。

注: 画面読み上げ機能を実行する必要がない場合は、画面読み上げ互換モードを選択しないでTrusteer Rapportを再インストールすることを強くお勧めします。

- [キャンセル]をクリックします。ポリシーの有効化をキャンセルする場合は、このオプションを選択します。

管理者モードからの再インストールアラートに対する応答

以下に、管理者モードからの再インストールアラートの例を示します。



このアラートは、Trusteer Rapportのプロバイダーが、RapportのインストールをWindows管理者アカウントからのみ実行できるように、最近になって制限をかけたことを示しています。ご使用のTrusteer Rapportは、標準ユーザーアカウントからインストールされています。プロバイダーは、以前Trusteer Rapportをインストールした際に使用した標準ユーザーアカウントを使用して、現在使用中のTrusteer Rapportをアンインストールし、その後管理者アカウントからTrusteer Rapportを再インストールすることをお奨めしています。いったんTrusteer Rapportを管理者アカウントからインストールすると、ご使用のコンピューターのすべてのユーザーアカウントで、Trusteer Rapportが有効になります。

Windows管理者アカウントとは、コンピューターの全ユーザーに影響する変更、または特定のユーザーに影響する変更を行うことができるWindowsユーザーアカウントです。これらの変更には、セキュリティ設定、ソフトウェアのインストール、ファイルへのアクセスなどが含まれます。すべてのWindowsコンピューターに管理者アカウントがありますが、マイクロソフト社では、日常的なコンピューターの運用では、標準ユーザーアカウントを使用することをお奨めしています。

このアラートが表示されたら、以下のいずれかを実行します。

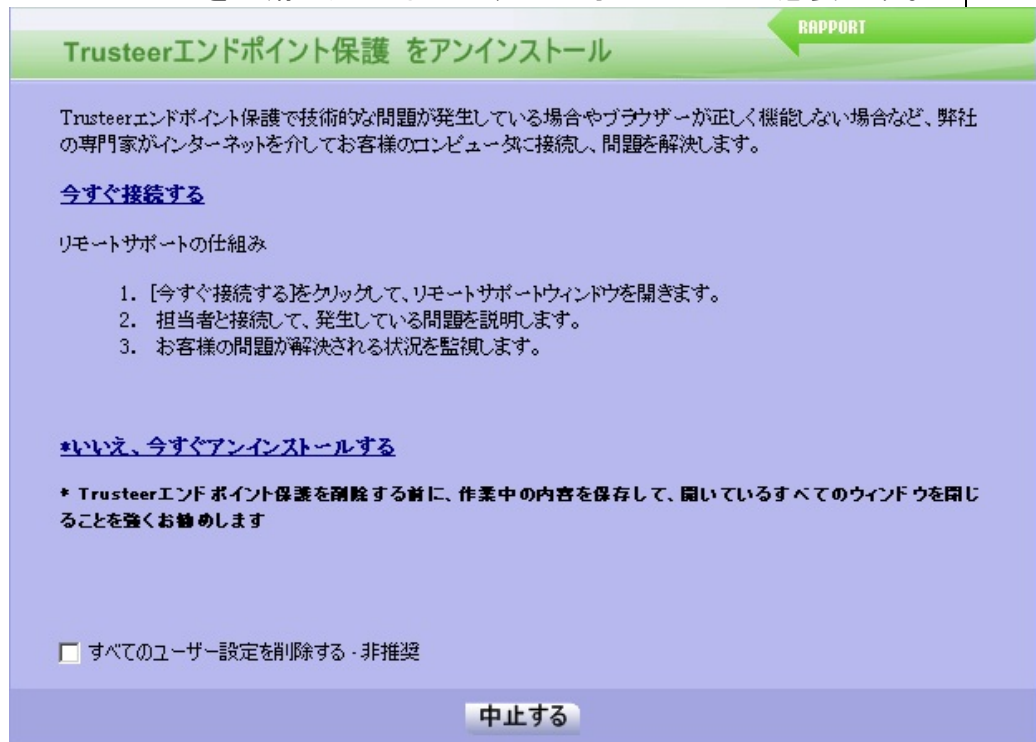
- [閉じる]をクリックします。アラートが閉じます。その後、以下の手順に従って推奨される再インストールを実行できます。
- [7日後に通知する]をクリックします。アラートが閉じます。7日後、再インストールを促すアラートが再度表示されます。

→ 推奨される再インストールの実行方法

1. Trusteer Rapportをインストールした際に使用した標準ユーザーアカウントを使用して、Trusteer Rapportをアンインストールします。

- [「Trusteer Rapport のアンインストール\(Windows 7\)」](#) (157ページ)
- [「Trusteer Rapport のアンインストール\(Windows XP\)」](#) (158ページ)

注: アンインストールする際、以下の画面で表示される[すべてのユーザー設定を削除する]チェックボックスはオンにしてください。再インストールを円滑に進めるには、このオプションが必要です。



2. 以下を参照して、管理者アカウントに切り替えます。

- [「管理者アカウントへの切り替え\(Windows 7\)」](#) (152ページ)

- [「管理者アカウントへの切り替え\(XP\)」](#) (154ページ)
 - [「管理者アカウントへの切り替え\(Vista\)」](#) (156ページ)
3. ご利用のプロバイダーの最新バージョンのTrusteer Rapportをダウンロードします。
- a. <http://www.trusteer.com/support/en/windows-operating-systems-xp-vista-windows-7>にアクセスします。
 - b. ご利用のプロバイダー(銀行、企業、またはその他の、ユーザーにTrusteer Rapportを提供した組織)に合わせて、適切なダウンロードリンクを見つけます。
 - c. プロバイダーのリンクをクリックして、インストールファイルをダウンロードします。
 - d. プロンプトが表示されたら、ファイルをコンピューターに保存します。
 - e. ファイルを実行してインストールします。インストール手順の詳細については、[「Trusteer Rapportのインストール」](#) (27ページ)を参照してください。

管理者アカウントへの切り替え(Windows 7)

管理者アカウントに切り替えるには、管理者ユーザーアカウントのユーザー名とパスワードが必要です。管理者ユーザーのユーザー名とパスワードが不明な場合は、管理者に問い合わせでご使用のアカウントタイプを変更するか、Trusteer Rapportをインストールする必要があります。

➔ 管理者ユーザーアカウントへの切り替え方法

1. [スタート]ボタンをクリックします。
2. [シャットダウン]ボタンの横にある矢印をクリックします。
3. [ユーザーの切り替え]をクリックします。

4. **Ctrl+Alt+Delete**を押してから、切り替え先のユーザー名をクリックします。

使用しているアカウントが管理者アカウントか不明な場合

アカウントが管理者アカウントか標準ユーザーアカウントか不明な場合は、そのアカウントに切り替えてから、以下の手順を実行して、アカウントタイプを確認します。

➔ ドメイン内のコンピューターの場合

1. [スタート]ボタンをクリックします。
2. [コントロールパネル]をクリックします。
3. [ユーザーアカウント]をクリックします。
4. [ユーザーアカウント]をクリックします。
5. [ユーザーアカウントの管理]をクリックします。
6. 管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けされない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名が強調表示され、アカウントタイプが[グループ]欄に表示されます。

➔ ワークグループ内のコンピューターの場合

1. [スタート]ボタンをクリックします。
2. [コントロールパネル]をクリックします。
3. [ユーザーアカウントと家族のための安全設定]をクリックします。
4. [ユーザーアカウント]をクリックします。

5. **[別のアカウントの管理]**をクリックします。管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けされない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名の下にアカウントタイプが表示されます。

管理者アカウントへの切り替え(XP)

管理者アカウントに切り替えるには、管理者ユーザーアカウントのユーザー名とパスワードが必要です。管理者ユーザーのユーザー名とパスワードが不明な場合は、管理者に問い合わせでご使用のアカウントタイプを変更するか、Trusteer Rapportをインストールする必要があります。

➔ 管理者ユーザーアカウントへの切り替え方法

- ユーザーの簡易切り替え機能が有効な場合(64 MB RAM以上のコンピュータで稼働しているWindows XP Home EditionまたはProfessionalではデフォルトで有効)
 1. **[スタート]**をクリックします。
 2. **[ログオフ]**をクリックします。
 3. **[ユーザーの切り替え]**をクリックします。Windows XPのログオン画面が表示され、各ユーザーのユーザー名の下に、実行しているプログラムの数が表示されます。
 4. 切り替え先のユーザー名をクリックします。
 5. パスワードを入力してから矢印ボタンをクリックして、コンピュータにログオンします。
- ユーザーの簡易切り替え機能が無効になっている場合またはサポートされていない場合(ドメインネットワークの一部であるWindows XP Professionalベースのコンピュータ)
 1. コンピューターを再起動します。

2. 管理者ユーザーのユーザー名およびパスワードを使用してログオンします。

使用しているアカウントが管理者アカウントか不明な場合

アカウントが管理者アカウントか標準ユーザーアカウントか不明な場合は、そのアカウントに切り替えてから、以下の手順を実行して、アカウントタイプを確認します。

➔ **ドメイン内のコンピューターの場合**

1. [スタート]ボタンをクリックします。
2. [コントロールパネル]をクリックします。
3. [ユーザーアカウント]をクリックします。
4. [ユーザーアカウント]をクリックします。
5. [ユーザーアカウントの管理]をクリックします。
6. 管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けられない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名が強調表示され、アカウントタイプが[グループ]欄に表示されます。

➔ **ワークグループ内のコンピューターの場合**

1. [スタート]ボタンをクリックします。
2. [コントロールパネル]をクリックします。
3. [ユーザーアカウントと家族のための安全設定]をクリックします。
4. [ユーザーアカウント]をクリックします。

5. **[別のアカウントの管理]**をクリックします。管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けされない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名の下にアカウントタイプが表示されます。

管理者アカウントへの切り替え(Vista)

管理者アカウントに切り替えるには、管理者ユーザーアカウントのユーザー名とパスワードが必要です。管理者ユーザーのユーザー名とパスワードが不明な場合は、管理者に問い合わせでご使用のアカウントタイプを変更するか、Trusteer Rapportをインストールする必要があります。

➔ 管理者ユーザーアカウントへの切り替え方法

1. **[スタート]**ボタンをクリックします。
2. **[ロック]**ボタンの横にある矢印をクリックします。
3. **[ユーザーの切り替え]**をクリックします。
4. 切り替え先のユーザーをクリックします。

使用しているアカウントが管理者アカウントか不明な場合

アカウントが管理者アカウントか標準ユーザーアカウントか不明な場合は、そのアカウントに切り替えてから、以下の手順を実行して、アカウントタイプを確認します。

➔ ドメイン内のコンピューターの場合

1. **[スタート]**ボタンをクリックします。
2. **[コントロールパネル]**をクリックします。
3. **[ユーザーアカウント]**をクリックします。
4. **[ユーザーアカウント]**をクリックします。
5. **[ユーザーアカウントの管理]**をクリックします。

6. 管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けされない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名が強調表示され、アカウントタイプが[グループ]欄に表示されます。

➔ ワークグループ内のコンピューターの場合

1. [スタート]ボタンをクリックします。
2. [コントロールパネル]をクリックします。
3. [ユーザーアカウントと家族のための安全設定]をクリックします。
4. [ユーザーアカウント]をクリックします。
5. [別のアカウントの管理]をクリックします。管理者パスワードまたは確認を求めるプロンプトが表示されたら、パスワードを入力するか、確認します(パスワードが受け付けされない場合、使用しているアカウントは標準ユーザーアカウントと考えられます)。ユーザー名の下にアカウントタイプが表示されます。

Trusteer Rapport のアンインストール(Windows 7)

➔ Trusteer Rapportのアンインストール方法

1. コントロールパネルを開きます。
2. [すべてのプログラム]の下にある[プログラムのアンインストール]をクリックします。
3. プログラムの一覧の中からTrusteer Rapportを見つけ、[Rapport]をダブルクリックします。確認メッセージが表示されます。
4. [はい]をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。

5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。
6. **[いいえ、今すぐアンインストールする]**をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

Trusteer Rapport のアンインストール(Windows XP)

➔ Trusteer Rapportのアンインストール方法

1. コントロールパネルを開きます。
2. **[アプリケーションの追加と削除]**をクリックします。
3. プログラムの一覧の中からTrusteer Rapportを見つけ、Trusteer Rapportに対する**[変更と削除]**ボタンをクリックします。確認メッセージが表示されます。
4. **[はい]**をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。
5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。

6. [いいえ、今すぐアンインストールする]をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

再起動を求めるアラートに対する応答

以下に、再起動を求めるアラートの例を示します。



このダイアログボックスは、Trusteer Rapportの一部の機能が更新され、その機能を有効にするには再起動が必要な場合に表示されます。以下のいずれかを実行します。

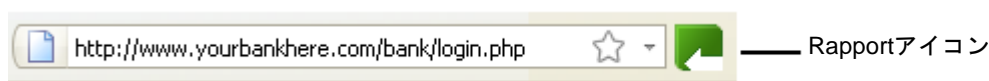
- [今すぐ再起動]をクリックします。コンピューターがただちに再起動されます。
- [後で通知する]をクリックします。ダイアログボックスが閉じます。後で、再度通知が表示されます。
- [キャンセル]をクリックします。ダイアログボックスが閉じます。この更新に関連する再通知を受け取ることは無くなります。次回コンピューターを再起動したときに、更新された機能が有効になります。

11.Trusteer Rapport のカスタマイズ

Rapportコンソールとダイアログボックスの言語を変更したり、ブラウザのアドレスバーの近くに表示されるTrusteer Rapportアイコンを非表示にしたり、システムトレイに表示されるTrusteer Rapportを非表示にしたりできます。

Trusteer Rapportのアドレスバーアイコンの表示/非表示

デフォルトでは、Trusteer Rapportアイコンは常にブラウザのアドレスバーの上または右端の近くに表示されます。このアイコンは、ブラウザに表示されているWebサイトがTrusteer Rapportによって保護されている場合は緑色、ブラウザに表示されているWebサイトがTrusteer Rapportによって保護されていない場合は灰色になります。



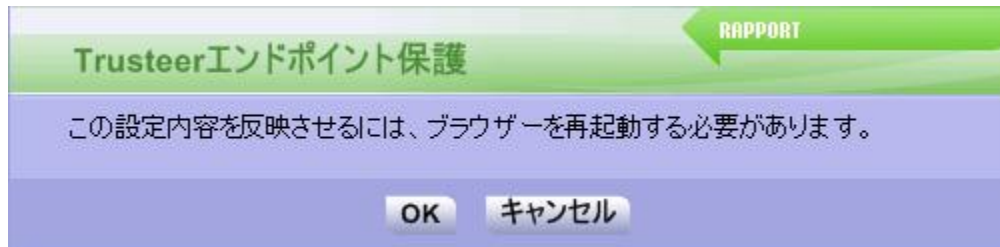
どのWebサイトが保護されているかを示す他にも、このアイコンを使用して、保護されていないWebサイトを保護することができます(Trusteer Rapportアイコンをクリックして[このWebサイトを保護する]を選択するだけ)。

Trusteer Rapportでは、このアイコンを表示したくない場合は非表示にすることができます。Trusteer Rapportアイコンが非表示でもTrusteer Rapportは保護されたWebサイトに対して同様の保護を提供します。ただし、どのWebサイトが保護されているかは判別できず、保護されていないWebサイトを保護するように選択することもできません。

アイコンの表示、非表示は、Rapportコンソールで制御されています。アイコンが非表示の場合は、WindowsのスタートメニューからでないとRapportコンソールにアクセスできません。

➔ Trusteer Rapportアイコンの非表示方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードの[設定]領域にある[アドレスバーアイコン]ステータスの横で、[非表示]をクリックします。メッセージボックスが表示されます。



3. [OK]をクリックします。[アドレスバーアイコン]ステータスが非表示に変更され、[表示する]ボタンが表示されます。



ブラウザーでただちに非表示になるか、ブラウザーの再起動後に非表示になります。

➔ アイコンの再表示方法

[表示する]をクリックします。

システムトレイアイコンの表示/非表示


デフォルトでは、Trusteer Rapportの実行中は、Trusteer Rapportアイコン()が常にシステムトレイに表示されます。



図1: システムトレイアイコン

このアイコンは、Trusteer Rapportのブラウザーに依存しない保護が機能していることを示しています。これには、マルウェアの防止、スキャン、駆除が含まれます。このアイコンを使用してRapportコンソールを開くこともできます (Trusteer RapportアイコンをクリックするだけでRapportコンソールが開きます)。

Trusteer Rapportでは、このアイコンを表示したくない場合は非表示にすることができます。システムトレイにTrusteer Rapportアイコンが表示されていない場合も、Trusteer Rapportは同様の保護を提供します。

アイコンの表示、非表示は、Rapportコンソールで制御されています。アイコンが非表示の場合は、WindowsのスタートメニューからでないとRapportコンソールにアクセスできません。

➔ システムトレイのTrusteer Rapportアイコンの非表示方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードの[設定]領域にある[トレイアイコン]ステータスの横で、
[非表示]をクリックします。[トレイアイコン]ステータスが非表示に変更
され、[表示する]ボタンが表示されます。



システムトレイのアイコンが非表示になります。

➔ アイコンの再表示方法

[表示する]をクリックします。

インターフェース言語の変更

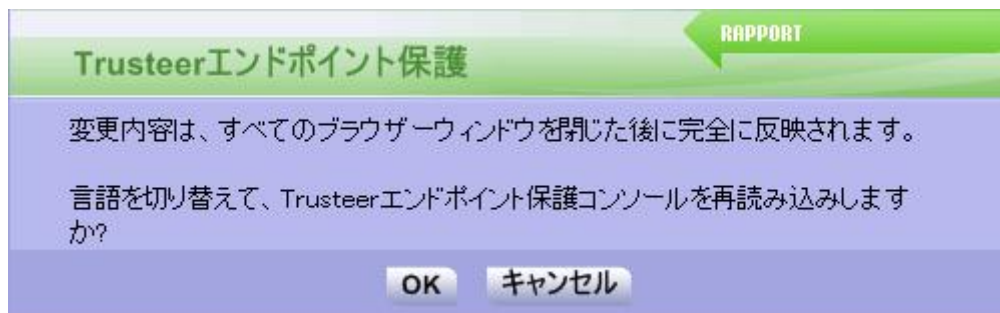
デフォルトでは、Trusteer RapportのRapportコンソールおよびその他のすべてのダイアログボックスは、英語のテキストで表示されます。Rapportコンソールおよびその他すべてのダイアログボックスで使用する言語を、スペイン語、フランス語、ドイツ語に変更できます。

➔ Rapportコンソールの言語変更方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードの[設定]領域で、[追加設定]をクリックします。[設定]タブが表示されます。



3. [言語]ドロップダウンリストから、言語を変更します。以下のメッセージが表示されます。



4. [OK]をクリックします。選択した言語でRapportコンソールがリロードされます。

The screenshot shows the Trusteer Rapport dashboard with a green header and a blue background. The main content is organized into four panels:

- 設定 (Settings):** Contains three checked items: 'Rapportは 実行中 (停止)', 'アドレスバーアイコン:表示 (非表示)', and 'トレイアイコン: 表示 (非表示)'. It also shows 'バージョン: Emerald Build 1302.31' and '保留中の更新: なし(最新の状態)'. A link for '追加設定' is at the bottom.
- 週次アクティビティレポート (Weekly Activity Report):** Features three input fields for 'ブロックされたスクリーンキャプチャー', '証明書の不一致', and 'ブロックされたIPアドレス', each with a '0' value. A link for 'フルレポート' is below.
- 信頼されたサイト (Trusted Sites):** Displays '信頼されたパートナーのウェブサイト 299' and '要注意ウェブサイト: 0'. A padlock icon is present, and a link for '信頼されたウェブサイトの閲覧' is at the bottom.
- ヘルプとサポート (Help and Support):** Lists links for '問題の報告', 'よく寄せられる質問', 'ユーザーガイド', and 'フィードバックを返す'. A question mark icon is on the right.

At the bottom, there is a '1 / 3 ページ' indicator and a green play button icon.

12.Trusteer Rapport のアクティビティの表示

Trusteer Rapportの保護メカニズムは、複数の異なるイベントタイプでトリガーされます。これらのイベントの一部は、マルウェアによって引き起こされるイベントに似た正規のイベントです。その他のイベントは、コンピューターに潜んでいるマルウェアによって開始されたイベントである可能性があります。各イベントはカウントされ、アクティビティレポートに記録されます。アクティビティレポートは、必要なときにいつでも確認できます。このレポートには、過去7日間のアクティビティが表示されます。このカウントをリセットまたは停止したり、各週の最初に画面に表示され、週次アクティビティレポートを表示するかを尋ねるダイアログボックスを有効または無効にしたりすることができます。

アクティビティレポートの表示

週次アクティビティレポートは、過去7日間において、各Trusteer Rapportの各メカニズムによりトリガーされたイベントの数を表示します。このレポートは情報提供のみを目的としています。Trusteer Rapportは、データを危険にさらすおそれのあるすべてのセキュリティイベントをブロックするため、ユーザーのアクションは必要ありません。アクティビティレポートは、Trusteer Rapportをインストールした12時間後に自動的に表示されます。

アクティビティレポートにイベントが含まれていても、必ずしもご使用のコンピューターにマルウェアが潜んでいる、または不正なWebサイトを閲覧したことを意味するものではありません。一部のソフトウェアや、閲覧したWebサイトの中に、保護されたWebサイトのオーナーまたはTrusteerのセキュリティポリシーに違反しているものがあることを意味しています。たとえば、銀行明細のスクリーンショットを作成するソフトウェアや、オンラインバンキングWebサイトに入力した情報を読み取ろうとするソフトウェアを、ユーザーが持っている場合があります。このポリシー違反により、Trusteer Rapportは、ソフトウェアが機密情報にアクセスすることをブロックしました。

➔ 週次アクティビティレポートを随時表示する方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードの[週次アクティビティレポート]で、[フルレポート]をクリックします。週次アクティビティレポートが表示されます。

Trusteer Rapport

ダッシュボード 週次アクティビティレポート

週次アクティビティレポート

このレポートには、Trusteerエンドポイント保護の最新のセキュリティアクティビティが示されています。詳細については、以下のセクションをクリックしてください。

このレポート内のイベント総数: 1

ブロックされたスクリーンキャプチャーイベント数: 1

以下のプロセスによって、保護されたWebサイトのイメージキャプチャーが試行されました。Trusteerエンドポイント保護により、これらスクリーンキャプチャーの試行がブロックされました。必ずしも、これらのプロセスに悪意があることを意味しません。アプリケーションによっては、通常の操作としてスクリーンショットを取得することもあります。お客様によるアクションは不要です。機密情報が表示される限り、スクリーンキャプチャーの試行に対してTrusteerエンドポイント保護はブロックを継続します。

- May 27 2013 17:38 MWSnap.exe is permanently blocked from capturing sensitive data

証明書不一致イベント数: 0

以下の保護されたWebサイトで不正な形式の証明書が示されました。Webサイトを正式に識別するための証拠が提示されません。お客様によるアクションは不要です。お客様が不正な形式の証明書を有する保護されたWebサイトにアクセスすると、Trusteerエンドポイント保護により警告が出され、お客様がアクセスをブロックできるようになります。

毎週初めに、このレポートを自動的に示す
このレポートの詳細については、[ここをクリック](#)

レポートをクリアする レポートを無効にする

このレポートでは、8つのイベントカテゴリに対する8つのカウンターが表示されます。アクティビティレポートのカテゴリには、ユーザーがインターネットをブラウズしている間にRapportが遭遇し、リスクを無効化した、さまざまなイベントタイプが一覧表示されます。

3. 各カウンター名をクリックすると、カウントしているセキュリティイベントについての説明、およびこのカテゴリでカウントされたイベントのリストが表示されます。

注: このレポートで表示される情報は若干技術的な内容であるため、イベントの一部またはすべてを理解できなくても、心配ありません。前述のように、この情報に対するユーザーのアクションは必要ありません。このレポートを閉じ、再度確認しなくても、安全は確保されています。このレポートは、これまでのTrusteer Rapportのアクティビティを検討したいユーザー向けに用意されています。

アクティビティレポートの設定

アクティビティレポートには、7日ごとに自動的に表示されるようにするオプションがあります。アクティビティレポートは、最初にTrusteer Rapportをインストールした12時間後に自動的に表示されます。デフォルトでは、レポートは毎週表示されるものではなく、必要なときにRapportコンソールで表示できるようになっています。

週次アクティビティレポートをクリアすると、すべてのイベントカウンターがクリアされます。週次アクティビティレポートを無効にすると、すべてのイベントカウンターが停止します。

➔ アクティビティレポートの設定方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードの[週次アクティビティレポート]領域で、[フルレポート]をクリックします。週次アクティビティレポートが表示されます。



ここで、以下の動作が可能です。

- [毎週初めに、このレポートを自動的に示す]チェックボックスをオンにして、週次アクティビティレポートを有効にします。7日ごとに、レポートを表示するかを尋ねるダイアログボックスが表示されます。
- レポートをクリアします。
- レポートを無効にします。

13. セキュリティ向上のためのコンピューターの スキャン

セキュリティ上、コンピューターのソフトウェアを最新の状態に保つことが重要です。新たな脅威は常に出現しており、ソフトウェア会社は定期的にプログラムを更新して、セキュリティの脆弱性やその他のバグを修正しています。ソフトウェアプログラムの中には、最新の状態でないと、特に悪用されやすいものがあります。


Trusteer Rapportは、3日ごとにコンピューターをスキャンし、コンピューターにアンチウィルスプログラムがインストールされていること、およびアンチウィルスプログラムやその他のさまざまなソフトウェアプログラム(たとえば、Adobe Flash、Adobe Reader、Java、Skypeなど)が、最新バージョンであることをチェックします。セキュリティ上のベストプラクティスレポートでは、Trusteer Rapportにより検出された、古くなっているプログラムと、その更新方法が通知されます。セキュリティ上のベストプラクティスレポートには、Rapportコンソールからアクセスできます。

手動スキャンの実行

Trusteer Rapportは定期的にスキャンを実行しますが、必要なときに随時再スキャンすることができます。

➔ セキュリティ向上のためにコンピューターをスキャンする方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

- ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、左下にセキュリティ上のベストプラクティスのサマリーが表示されます。



The screenshot shows the Trusteer Rapport dashboard with the following sections:

- セキュリティポリシー**: 有効: 19 セキュリティコントロール, 無効: 1 セキュリティコントロール, 編集: 0 (Default settings). Includes a link for [ポリシーの編集 \(アドバンスドユーザー向け\)](#).
- パフォーマンスおよび接続性**: Trusteer (0%), システム (22%). Includes a link for [インターネット接続: 自動 \(変更する\)](#).
- セキュリティ上のベストプラクティス**: 最終スキャン結果のサマリー. Includes a warning icon and text: **セキュリティ上のベストプラクティスを順守していますか?**, **考慮すべき5件の改善点**. Includes links for [レポートを表示する](#) and [もう一度スキャンする](#).
- OTPアカウント**: OTPアカウント管理: OTPアカウントを管理する. 0件の有効なアカウントがあります. Includes a link for [OTPアカウントを管理する](#).


Page navigation: 2 / 3 ページ

- ダッシュボードの[セキュリティ上のベストプラクティス]領域で、[もう一度スキャンする]をクリックします。このスキャンの実行中は、[もう一度スキャンする]ボタンが消え、[スキャン中です...]という文字が表示されます。スキャンが終了すると、[もう一度スキャンする]が再表示され、スキャン結果が更新されます。

セキュリティ上のベストプラクティスレポートの表示

セキュリティ上のベストプラクティスレポートでは、Trusteer Rapportにより検出された、古くなっているプログラムと、その更新方法が通知されます。

➔ セキュリティ上のベストプラクティスレポートの表示方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、左下にセキュリティ上のベストプラクティスのサマリーが表示されます。

最終スキャン
結果の
サマリー



The screenshot shows the Trusteer Rapport dashboard with a green header and a blue background. The main content is divided into four panels:

- セキュリティポリシー (Security Policy):** Shows 19 active security controls and 1 inactive control. It includes a link to edit policies.
- パフォーマンスおよび接続性 (Performance and Connectivity):** Displays progress bars for Trusteer (0%) and システム (System, 22%). It also shows internet connection status as automatic.
- セキュリティ上のベストプラクティス (Security Best Practices):** Asks if best practices are followed and highlights 5 areas for improvement. It includes links to view the report and rescan.
- OTPアカウント (OTP Accounts):** Shows 0 active accounts and a link to manage them.

Navigation arrows and a page indicator '2 / 3 ページ' are visible at the bottom.

3. [レポートを表示する]をクリックします。セキュリティ上のベストプラクティスレポートが表示され、スキャンにより検知されたセキュリティ問題のレポートが示されます。

検出された
セキュリティ
の問題



4. 各セキュリティ問題をクリックします。その問題により引き起こされるリスクについての詳細説明と、その問題に対して推奨されるアクションが表示されます。

The screenshot shows the Trusteer Rapport interface. At the top, there's a green header with the title 'Trusteer Rapport'. Below it, a navigation bar contains 'ダッシュボード' and 'セキュリティ上のベストプラクティス'. The main content area is titled 'セキュリティ上のベストプラクティス' and contains a paragraph of introductory text. Below this, there are two alert boxes. The first alert is for 'Google Chrome Internetブラウザが最新ではありません'. It includes a 'リスクの説明' section with detailed text about Chrome's security vulnerabilities and a '改善のための推奨事項' section with instructions on how to update. The second alert is for 'Mozilla Firefoxが最新ではありません', also with a 'リスクの説明' section. A callout box on the right side of the screenshot points to the alert titles with the text '問題をクリックすると、この詳細が表示される'.

問題をクリック
すると、この詳細が
表示される

14. セキュリティニュースの受信

セキュリティニュースセンターは、オンライン上での安全確保について発信されるTrusteerからの重要なメッセージを受信するための個人用スペースです。Trusteerはセキュリティニュースセンターを使用して、ユーザーへのお知らせや、新たに出現した攻撃についての情報および回避方法のアドバイスを送信します。セキュリティニュースセンターは完全にフィッシングやスパムを排除しており、未承認のメッセージを受信することはありません。


セキュリティニュースセンターのメッセージは、複数の異なるチャンネルに分類されます。ユーザーは自動的に2つのチャンネルを購読するように設定されています。どちらのチャンネルも、ユーザーがオンライン上で安全を確保するために必要なデータを提供することを目的としています。

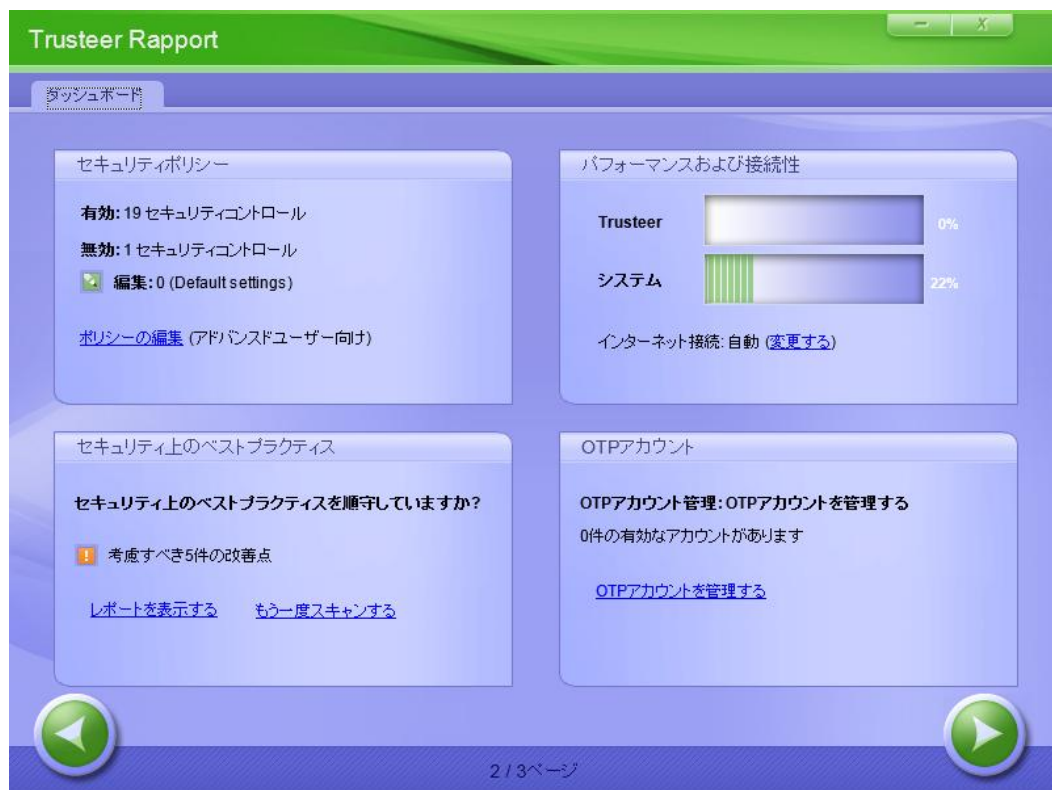
- **[Trusteer]:** セキュリティを向上するために、Trusteer Rapportソフトウェアをより有効活用するためのヒント。
- **[脅威情報を更新する]:** 新たなセキュリティ上の脅威についての更新情報と、安全にWebサーフィンを行う上で役立つアドバイス。

セキュリティニュースセンターの表示

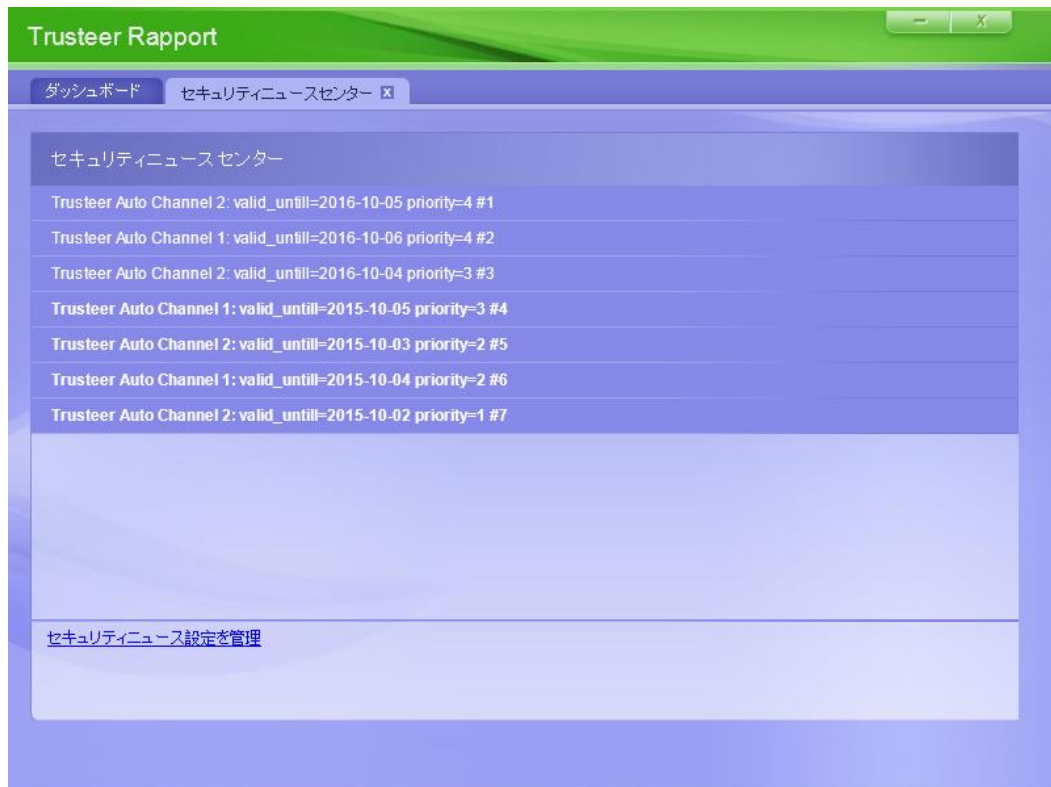
セキュリティニュースセンターには、Rapportコンソールからアクセスできません。

➔ セキュリティニュースセンターの表示方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、右下にセキュリティニュースセンターのサマリーが表示されます。




3. [セキュリティニュースを表示する]をクリックします。セキュリティニュースセンターが表示されます。




セキュリティニュースチャンネルの購読

ユーザーは、自動的に[Trusteer]チャンネルおよび[脅威情報を更新する]チャンネルを購読するように設定されています。

➔ セキュリティニュースチャンネルの購読方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、右下にセキュリティニュースのサマリーが表示されます。



The screenshot shows the Trusteer Rapport dashboard with the following sections:

- セキュリティポリシー** (Security Policy):
 - 有効: 19 セキュリティコントロール (Active: 19 Security Controls)
 - 無効: 1 セキュリティコントロール (Inactive: 1 Security Control)
 - 編集: 0 (Default settings) (Edit: 0)
 - [ポリシーの編集 \(アドバンスドユーザー向け\)](#) (Edit Policy (Advanced User Only))
- パフォーマンスおよび接続性** (Performance and Connectivity):
 - Trusteer: 0%
 - システム: 22%
 - インターネット接続: 自動 ([変更する](#)) (Internet Connection: Automatic (Change))
- セキュリティ上のベストプラクティス** (Security Best Practices):
 - セキュリティ上のベストプラクティスを順守していますか? (Are you following security best practices?)
 - 考慮すべき5件の改善点 (5 areas for improvement)
 - [レポートを表示する](#) (View Report) | [もう一度スキャンする](#) (Rescan)
- OTPアカウント** (OTP Accounts):
 - OTPアカウント管理: OTPアカウントを管理する (OTP Account Management: Manage OTP Accounts)
 - 0件の有効なアカウントがあります (0 valid accounts)
 - [OTPアカウントを管理する](#) (Manage OTP Accounts)

At the bottom of the dashboard, there are navigation arrows and a page indicator: 2 / 3 ページ.

3. [セキュリティニュースを管理する]をクリックします。[セキュリティニュースチャンネル]画面が表示され、利用できるチャンネルが示されます。




4. 購読する各チャンネルの横にある[有効]を選択します。

通知の購読

セキュリティニュースセンターの通知を購読すると、セキュリティニュースセンターのメッセージが着信したときに、随時画面に通知メッセージが表示されます。

→ 通知の購読方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、右下にセキュリティニュースセンターのサマリーが表示されます。
3. [セキュリティニュースを管理する]をクリックします。[セキュリティニュースチャンネル]タブが表示されます。



4. [セキュリティニュースで新しいメッセージがあるときに通知する] チェックボックスをオンにします。これで、通知が有効になりました。

15.保護されたサイトおよびパスワードの管理

Trusteer Rapportでは、Rapportコンソールで、どのWebサイトおよびパスワードが保護されているかについての情報を確認できます。ユーザーは、RapportコンソールでWebサイトおよびパスワードを削除できます。

保護されたWebサイトの管理

保護されたWebサイトには、以下の2つのカテゴリがあります。

- **[信頼されたパートナーWebサイト]:** Trusteerのパートナーが所有するWebサイトです。信頼されたパートナーは、Trusteerと直接連携して、そのパートナーのアプリケーションに最適なセキュリティポリシーを提供しています。パートナーのWebサイトにアクセスするときは、自動的に保護されます。これらのWebサイトからTrusteer Rapportの保護を削除することはできません。保護されたパートナーWebサイトの数により、ご使用のコンピューターに負荷がかかることはありません。
- **[手動で追加したWebサイト]:** ユーザー自身が追加したWebサイトであり、これらのサイトに接続したときに、Trusteer Rapportによる保護を活用することを意図したものです。これらのWebサイトは、リストから削除することにより、Trusteer Rapportの保護を削除できます。

注: 一部のTrusteer Rapportのインストールでは、手動でWebサイトを保護する機能が無効になっています。

注: ご使用のTrusteer Rapportのライセンスでは、多数のWebサイトを追加することが許可されています。別のWebサイトでTrusteer Rapportの保護を有効にするために、既存のWebサイトを削除する必要はありません。ライセンスで許可されている数以上のWebサイトを保護する場合は、[「Trusteer Rapportのアップグレードのプロンプトに対する応答」](#) (147ページ)を参照してTrusteer Rapportをアップグレードできます。アップグレードは無償です。

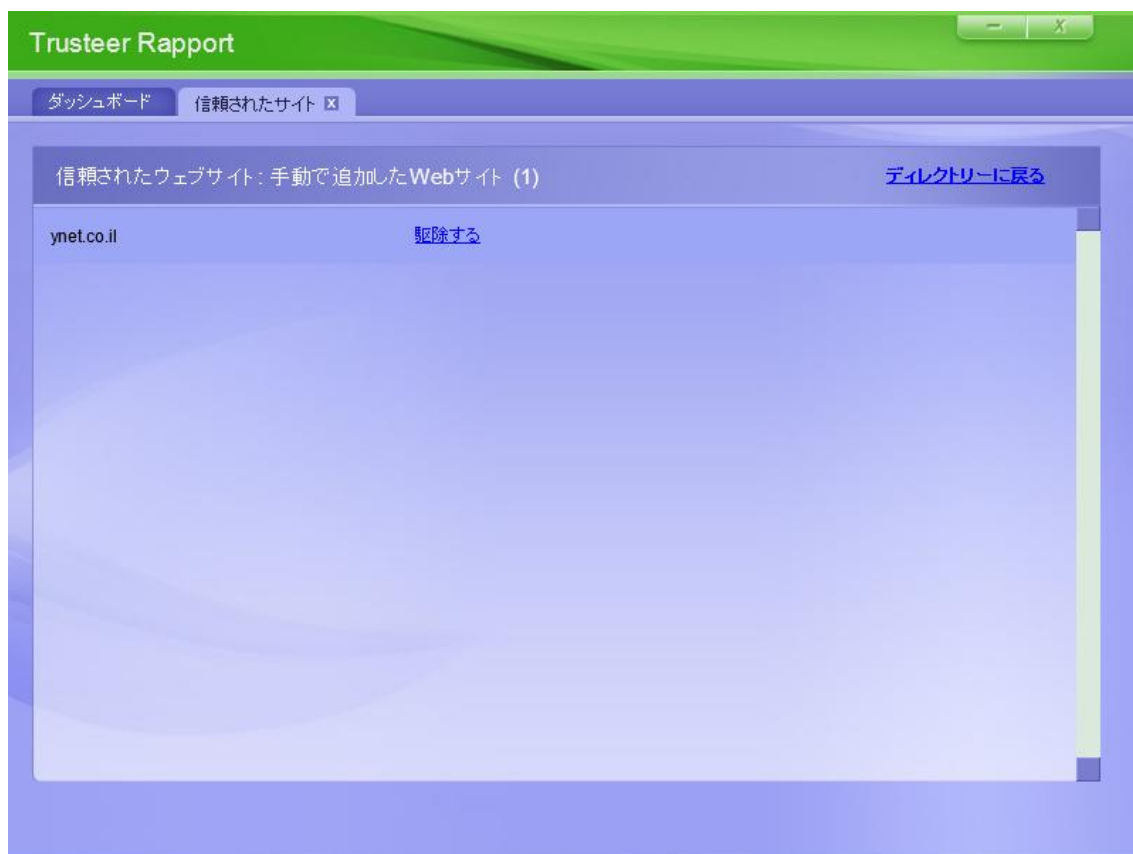
Rapportコンソールの[信頼されたWebサイト]領域には、現在各カテゴリで保護されているWebサイトの数が表示されます。[保護されたWebサイト]をクリックすると、保護されているパートナーWebサイトの説明の一覧を表示できます。[手動で追加したWebサイト]をクリックすると、手動で追加したWebサイトの一覧を表示できます。

➔ 手動で追加したWebサイトの削除方法

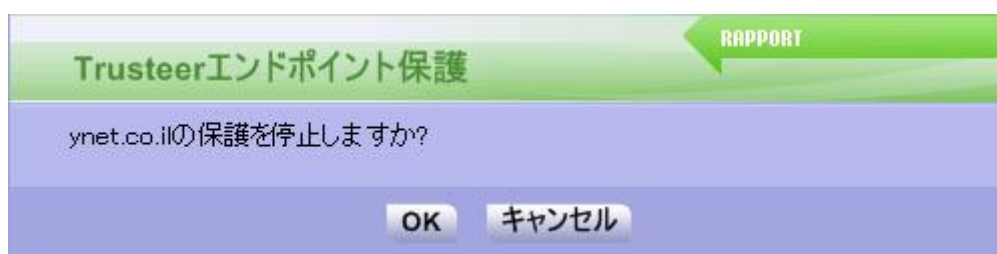
1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. [信頼されたWebサイト]領域で、[信頼されたウェブサイトの閲覧]をクリックします[信頼されたWebサイト]タブが表示されます。



3. [手動で追加したWebサイト]をクリックします。手動で追加されたすべてのWebサイトの一覧が表示されます。



4. リスト内のWebサイトの横にある[駆除する]リンクをクリックします。確認ボックスが表示されます。




5. [OK]をクリックします。Webサイトがリストから削除されます。次回、リストから削除されたWebサイトをブラウズすると、Trusteer Rapport アイコンは灰色で表示されます。これは、そのサイトが保護されていないことを意味しています。

保護されたユーザー名およびパスワードの管理

保護されたサイトでのパスワードを保護するTrusteer Rapportからの提案を承認した後は、Trusteer Rapportは当該のパスワードだけでなく、今後そのサイトで使用されるすべてのパスワードも保護します。Trusteer Rapportは、各Webサイト上でパスワードを保護する、または保護しないというユーザーの選択を記憶するため、ユーザーがパスワード保護キャッシュをクリアしない限り、次回以降そのサイトをブラウズしたときに、パスワード保護を促すことはありません。Rapportコンソールには、現在Trusteer Rapportのパスワード保護が有効になっているWebサイトが表示されます。必要に応じて、任意の保護されたWebサイトでのパスワード保護を無効にできます。また、パスワード保護のキャッシュをクリアして、すべてのパスワード保護、および保護する/しないの選択をクリアすることができます。

注: 一部のTrusteerのパートナーWebサイトでは、Trusteer Rapportにより、パスワードだけでなくユーザー名も保護されます。また、Rapportコンソールには、各Webサイトのユーザー名保護ポリシーも表示されます。

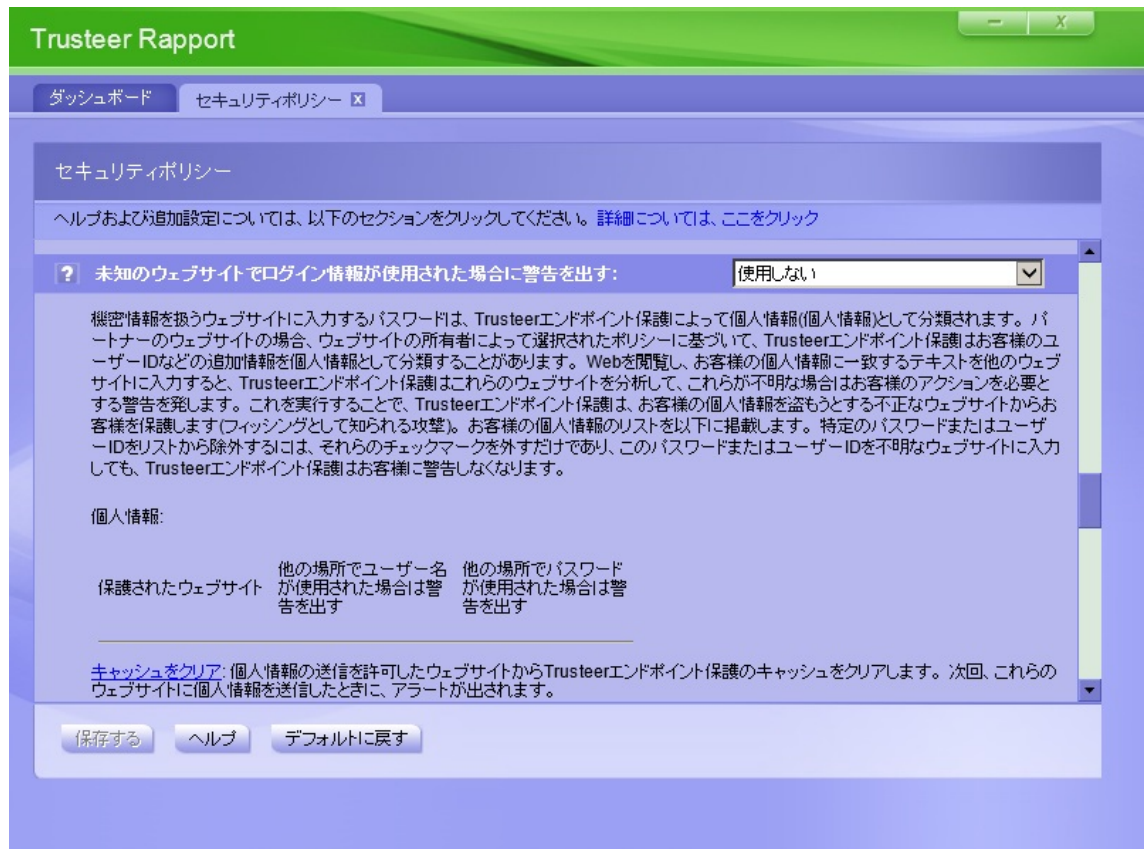
➔ 保護されたWebサイトのパスワード保護の無効化方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。
5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。ここには、すべてのセキュリティコントロールが表示されています。

6. セキュリティコントロールのリストを下にスクロールして、[未知のWebサイトでログイン情報が使用された場合に警告を出す]を見つけます。
7. [未知のWebサイトでログイン情報が使用された場合に警告を出す]をクリックします。各Webサイトのユーザー名およびパスワードに対する保護ポリシーが表示されます。



8. パスワード保護を無効にするWebサイトに対する[他の場所でパスワードが使用された場合は警告を出す]チェックボックスをオフにします。Trusteer Rapportによる当該のWebサイトのパスワード保護が解除されます。

注: [キャッシュをクリアする]をクリックすると、すべてのパスワード保護がクリアされ、すべてのパスワード保護ポリシーがリセットされます。これにより、次回各Webサイトにアクセスした際に、Trusteer Rapportによりパスワード保護を促すメッセージが再度表示されるようになります。

9. [保存する]をクリックします。変更内容が保存されます。

16.Trusteer Rapport のセキュリティポリシーの変更

注: 本項は、熟練したユーザー向けです。


Trusteer Rapportのセキュリティ機能では、ユーザーによる設定は必要ありませんが、必要に応じて変更できる機能が多数あります。

セキュリティポリシーサマリーの表示

Rapportコンソールには、セキュリティポリシーのサマリーが表示されます。このサマリーには、セキュリティポリシーコントロールがいくつ有効になっており、いくつ無効になっているかが示されます。

➔ セキュリティポリシーの表示方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。2つ目のダッシュボード画面が表示され、[セキュリティポリシー]領域にセキュリティポリシーのサマリーが表示されます。

セキュリティポリシーのサマリー



セキュリティポリシーのサマリーには、以下の情報が含まれます。

表示フィールド	説明
[有効]	現在有効なセキュリティコントロールの数
[無効]	現在無効なセキュリティコントロールの数
[編集]	デフォルトのポリシーから変更した数


セキュリティコントロールの変更

Trusteer Rapportのセキュリティポリシーでは、正規のプログラムとの衝突の可能性を最小限に抑えながら、最適なセキュリティが提供されます。たとえば、スクリーンキャプチャーのブロック機能は、パートナーWebサイトのみ保護するようにデフォルト設定されています。これは、画面をキャプチャーする正規の製品が数多く存在しており、Trusteerでは、オンラインバンキングまたは企業のセキュリティにとって非常に重要な場合のみ、この機能をブロックすることが望ましいと考えているためです。

Trusteer Rapportでは、ユーザーが各セキュリティコントロールを変更することで、セキュリティポリシーを変更できます。セキュリティポリシーを変更することで、デフォルトのセキュリティポリシーではブロックされてしまう正規のタスクを有効にしたり、その他のセキュリティアプリケーションとの互換性の問題を解決したりするのに役立つ場合があります。デフォルトのポリシーを変更すると、ほとんどの場合は、Trusteer Rapportが提供する保護のレベルが下がります。変更に伴うリスクについて十分理解してから、変更を行ってください。

注: Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしていないと変更できないポリシーがあります。

➔ セキュリティコントロールの変更方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。ここには、すべてのセキュリティコントロールが表示されています。



6. 変更するコントロールの右側にあるドロップダウンメニューで、目的の設定を選択します。変更を行う前に、その変更によって、Trusteer Rapportから提供される保護のレベルにどのような影響があるかを必ず確認し理解してください。セキュリティポリシーコントロール、使用できるオプション、および関連情報については、[「セキュリティポリシーコントロールについて」](#) (194ページ)を参照してください。以下に、表示される設定を示します。

- [常に]: コントロールはWebサイトに依存せず、常に有効です。
- [しない]: コントロールは常に無効です。
- [パートナーWebサイト上]: コントロールはパートナーWebサイトのオーナーが設定したポリシーに基づいて、パートナーWebサイトに対して有効です。パートナーWebサイトは、Trusteerと直接連携しており、非常に適切なセキュリティポリシーを提供しています。

- [パートナーおよびお客様の機密情報のWebサイト上]: パートナー Webサイトおよびユーザーが追加したWebサイト(「[追加のWebサイト保護](#)」(70ページ)を参照)でこのコントロールを使用できます。

各コントロール名をクリックすると、コントロールの説明と、そのコントロール固有の機能の説明が表示されます。

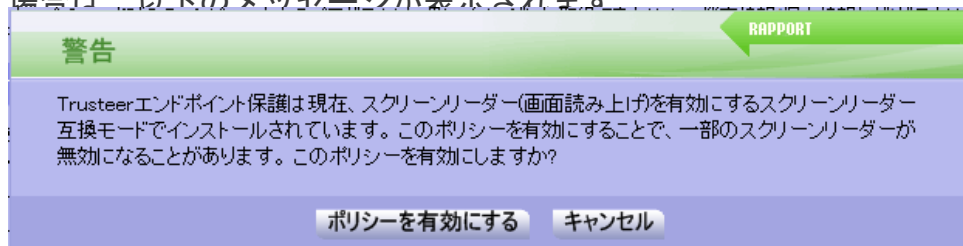


すべての設定をデフォルト値に戻す場合は、[デフォルトに戻す]をクリックします。

注: Trusteer Rapportを視覚障害モードでインストールしている場合、[スクリーンキャプチャーをブロックする]および[ブラウザー内の情報へのアクセスをブロックする]は[しない]に設定されています。

7. [保存する]をクリックします。ポリシーの変更が保存されます。変更を有効にするために、ブラウザーまたはコンピューターの再起動が必要な場合もあります。

注: Trusteer Rapportを画面読み上げ互換モードでインストールしており、[スクリーンキャプチャーをブロックする]ポリシーまたは[ブラウザ内の情報へのアクセスをブロックする]ポリシーを有効にした場合は、以下のメッセージが表示されます。



ポリシーの有効化を進める場合は、[ポリシーを有効にする]をクリックしてください。ポリシーの有効化が望ましくない場合(画面読み上げ機能を無効にしたい場合)は、[キャンセル]をクリックします。

セキュリティポリシーコントロールについて

Rapportのセキュリティポリシーを変更する前に、変更によってTrusteer Rapportの保護にどのような影響があるかを理解しておく必要があります。以下の表に、セキュリティポリシーコントロール、使用できるオプション、および関連情報を示します。

コントロール	説明	ポリシーオプション	追加情報
[スクリーンキャプチャーをブロックする]	<p>保護されたWebサイトがブラウザに表示されている間、あらゆるスクリーンキャプチャーの試行を無効にします。コンピューター上のプログラムで画面をキャプチャーしようとする、黒い画像が生成されません。</p> <p>この機能は、マルウェアが画面をキャプチャーし、機密情報を詐取しないよう防止することを目的としています。</p>	<ul style="list-style-type: none"> • [しない]: 常時スクリーンキャプチャーを許可します(このポリシーが[しない]に設定されている場合でも、Trusteer Rapportの停止などの特定の操作により表示されるセキュリティ確認メッセージはキャプチャーできません)。 • [パートナーのWebサイト上] (デフォルト): ブラウザーでパートナーのWebサイトが開いている間のみ、すべてのスクリーンキャプチャーをブロックします。 • [パートナーおよびお客様の機密情報のWebサイト上]: ブラウザーで保護されているWebサイト(パートナーのWebサイトまたは手動で追加したWebサイト)が開いている間のみ、すべてのスクリーンキャプチャーをブロックします。 	<p>Print Screenコマンドボタンは、その他のスクリーンキャプチャーメカニズムとは別に処理されます。Print Screenコマンドボタンを押すと、Trusteer Rapportは[プリントスクリーン検知]アラート(「[プリントスクリーン検知]アラートに対する応答」 (132ページ)を参照)を表示し、キャプチャーをブロックするか可能にするかを選択するよう促されます。</p> <p>コンピューター上で画面をキャプチャーする必要がある場合でも、この機能を無効にする必要はありません。Trusteer Rapportのキャプチャーブロック機能は、保護されたWebサイトが表示されていないときに、スクリーンキャプチャーメカニズムによる任意の画面のキャプチャーを阻止することはありません。デフォルトではスクリーンキャプチャーのブロック機能は保護されたパートナーWebサイトのみに適用されています。スクリーンキャプチャーがブロックされた場合でも、キーボードのPrint Screenコマンドボタンを使用すれば、画面をキャプチャーすることができます。この場合、Trusteer Rapportダイアログボックスが表示され、スクリーンキャプチャーをブロックするか、可能にするかを尋ねられます。ここで[許可]をクリックすれば、スクリーンキャプチャーが完了します。</p> <p>そのため、スクリーンキャプチャーのブロック無効化は、表示されているパートナーのWebサイトを、キーボードのPrint Screenコマンドボタンを使用する以外のスクリーンキャプチャーメカニズムを使用してキャプチャーする</p>

コントロール	説明	ポリシーオプション	追加情報
			<p>必要がある場合のみに限られます。画面のキャプチャーが完了したら、スクリーンキャプチャーブロック機能を再度有効にして、この機能によって提供されている保護を元に戻すことができます。</p> <p>Trusteer Rapportにより、保護されたWebサイト以外の画面でキャプチャーがブロックされる場合は、開いているすべてのブラウザを最小化するか、保護されたWebページが含まれるウィンドウまたはタブをすべて閉じます。これにより、ブロックされずに画面をキャプチャーできます。</p>
<p>[WebサイトのSSL証明書を検証する]</p>	<p>保護されたWebサイトをブラウザすると、Trusteer Rapportにより、そのWebサイトのSSL証明書がチェックされます。証明書が古い、間違っている、または不明な発行者によって署名されている場合、Trusteer Rapportは無効な証明書の警告(「無効な証明書の警告への応答」(141ページ)を参照)を発生し、ユーザーのアクションを求めます。Trusteer RapportのSSL証明書検証機能は、ブラウザ独自の検証メカニズムよりも強力であり、ブラウザにより無効な証明書の警告が表示される場合でも、パートナーWebサイト上では使用する必要があります。この機能は、ユー</p>	<ul style="list-style-type: none"> • [しない]: WebサイトのSSL証明書をチェックしません。 • [パートナーのWebサイト上] (デフォルト): パートナーのWebサイトにアクセスしたときに、そのサイトで使用されているSSL証明書をチェックします。 • [パートナーおよびお客様の機密情報のWebサイト上]: パートナーのWebサイトおよび手動で追加したWebサイトにアクセスしたときに、そのサイトで使用されているSSL証明書をチェックします。 	<p>無効な証明書の警告に対する応答方法の詳細については、「無効な証明書の警告への応答」(141ページ)を参照してください。</p> <p>以前承認してしまった無効な証明書から、Trusteer Rapportのキャッシュをクリアすることができます。キャッシュをクリアした後は、キャッシュから削除された証明書を使用しているWebサイトにアクセスすると、警告が表示されます。</p> <p>無効な証明書のキャッシュをクリアするには、[WebサイトのSSL証明書を検証する]ドロップダウンリストの下にある、[キャッシュをクリアする]をクリックします。</p>

コントロール	説明	ポリシーオプション	追加情報
	<p>ザーが不正なWebサイトにアクセスしないよう防止することを目的としています。</p>		
[未知のブラウザアダオンをブロックする]	<p>認識されていないブラウザアダオンをブロックします。ブラウザアダオン(ツールバーまたはBHOとも呼ばれる)は、ブラウザ内に組み込まれる小さな(通常はサードパーティー製)ソフトウェアで、ブラウザの通信をコントロールするものです。ほとんどのブラウザアダオン(Google ツールバーなど)は正規のものです。不正なアダオンもあります。</p> <p>この機能は、ログイン情報を盗んだり、通信を改ざんしたりするおそれのある悪意のあるブラウザアダオンから、ユーザーを保護することを目的としています。</p>	<ul style="list-style-type: none"> • [しない]: すべてのサイトでブラウザアダオンを許可します。 • [パートナーのWebサイト上]: パートナーWebサイトに接続している間、認識されていないブラウザアダオンをブロックします。 • [パートナーおよびお客様の機密情報のWebサイト上] (デフォルト): パートナーWebサイトおよび手動で保護しているWebサイトに接続している間、認識されていないブラウザアダオンをブロックします。 	<p>コンソールには、保護されたWebサイトに接続している間にTrusteer Rapportにより検知された、不明なアダオンのリストが表示されます。安全であることが分かっている特定のアダオンについて、各アダオンの[許可]チェックボックスをオンにすることで、手動でブロックを解除できます。</p>
[ブラウザ内の情報へのアクセスをブロックする]	<p>DOMプログラミングインターフェース(API)を使用してWebサイトにアクセスする、コンピューターのプロセスをブロックします。このようなプロセスは、機密情報を読み取ったり、トランザクションを改ざんし</p>	<ul style="list-style-type: none"> • [しない]: プロセスがWebサイトにアクセスすることをブロックしません。 • [パートナーのWebサイト上] (デフォルト): パートナーWebサイトに接続している間、プロセスをブロックします。 	<p>一般的な例としては、ログインWebサイトにおいて、パスワードを記憶したり、自動的に入力したりするパスワードマネージャーがあります。この情報は機密性が高いため、また、マルウェアによってソフトウェアが悪用されて金融Webサイトの認証情報が詐取されるおそれがあるため、Trusteer Rapportは、この機能が情報にアクセスするのをブロックします。オンラインの金融Webサイトで、そのような機能を使用することは、お奨めできません。正規</p>

コントロール	説明	ポリシーオプション	追加情報
	<p>たりするおそれがあります。Trusteer Rapportは、そのプロセスが正規であるか悪意のあるものであるかにかかわらず、これらのプロセスをブロックします。</p> <p>この機能は、悪意のあるプロセスにより、不正に機密情報が読み取られたり、トランザクションが改ざんされたりしないよう防止することを目的としています。</p>	<ul style="list-style-type: none"> • [パートナーおよびお客様の機密情報のWebサイト上]: パートナーWebサイトおよび手動で保護しているWebサイトに接続している間、プロセスをブロックします。 	<p>プログラムでも、パートナーのWebサイト上でこの情報にアクセスしようとして、Trusteer Rapportによりブロックされる場合があります。</p>
<p>[機密情報を扱うWebサイトのクッキーへのアクセスをブロックする]</p>	<p>パートナーWebサイトのオーナーが機密クッキーとして設定した、セッションクッキーなどのクッキーにアプリケーションがアクセスすることをブロックします。</p> <p>この機能は、セッションクッキーが悪用され、Webサイトとのセッションが乗っ取られないよう防止することを目的としています。</p>	<ul style="list-style-type: none"> • [しない]: アプリケーションがWebサイトにアクセスすることをブロックしません。 • [パートナーのWebサイト上] (デフォルト): パートナーWebサイトに接続中、機密クッキーへのアクセスをブロックします。 	<p>Trusteerは、Webサイトのクッキーを保護するようにTrusteer Rapportを設定する前に、そのクッキーについて熟知している必要があります。そうしないと、Webサイトとの機能衝突が発生するおそれがあります。このため、この保護タイプは、パートナーWebサイトでしか使用できません。</p>
<p>[Web サイトIPアドレスを検証する]</p>	<p>信頼されているIPアドレス変換テーブルと照合して、WebサイトIPアドレスを検証します。保護されたWebサイトにアクセスすると、Rapportにより、そのWebサイトのIPアドレスと、そ</p>	<ul style="list-style-type: none"> • [しない]: WebサイトIPアドレスと信頼されているIPアドレステーブルの照合チェックを行いません。 • [パートナーのWebサイト上]: パートナーWebサイトに接続する場合に、WebサイトIPアド 	<p>この機能では、現在キャッシュのクリア機能はサポートされていません。</p>

コントロール	説明	ポリシーオプション	追加情報
	<p>のWebサイトに対する既知の問題ないアドレスのリストが照合されます。リストで対象のIPアドレスが見つからない場合、Trusteer Rapportにより、そのIPアドレスは対象Webサイトの既知の問題ないIPアドレスに変更されます。</p> <p>この機能は、ファージング攻撃⁵による、不正なWebサイトへの接続を防止することを目的としています。</p>	<p>レスと信頼されているIPアドレステーブルの照合チェックを行います。</p> <ul style="list-style-type: none"> • [パートナーおよびお客様の機密情報のWebサイト上] (デフォルト): パートナーWebサイトおよび手動で保護されたWebサイトに接続する場合に、WebサイトIPアドレスと信頼されているIPアドレステーブルの照合チェックを行います。 	
<p>[キーロギングをブロックする]</p>	<p>ブラウザに入力されるキーストロークをすべて暗号化して、キーロガーと呼ばれる悪意のあるプログラムからキーストロークを隠します。</p> <p>この機能は、キーロガーによりキーストロークが読み取られ、パスワードなどの機密情報が詐取されないよう防止することを目的としています。</p>	<ul style="list-style-type: none"> • [しない]: キーロギングをブロックしません。 • [パートナーのWebサイト上]: パートナーWebサイトに接続している間、キーロギングをブロックします。 • [パートナーおよびお客様の機密情報のWebサイト上] (デフォルト): パートナーWebサイトおよび手動で保護しているWebサイトに接続している間、キーロギングをブロックします。 	<p>この機能は、その他のアンチキーロガーと機能衝突し、キーストロークがスクランブル化される場合があります。そのため、別のキーロガーを実行している場合(ご使用のアンチウイルスソフトウェアに組み込まれている場合など)は、この機能を無効にする必要があります。または、既存のソフトウェアのキーロギング保護を無効にすることもできます。</p> <p>このポリシーを無効にした覚えが無いにもかかわらず、ポリシーが無効になっている場合は、Trusteer Rapportが、ご使用のハードウェアまたはソフトウェアの設定と、Trusteer Rapport間の機能衝突を検知したことを意味します。Trusteer Rapportは、衝突を避けるために、このメカニズムを無効にしています。</p>

⁵ ファージング攻撃は、Webサイトトラフィックを、偽のWebサイトにリダイレクトしようとする行為を指します。

コントロール	説明	ポリシーオプション	追加情報
[感染する可能性のあるサイトをブラウザしたときに警告を出す]	コンピューターにマルウェアを感染させるWebサイトにアクセスしようとした場合、ユーザーに警告します。	<ul style="list-style-type: none"> • [しない]: 警告を表示しません。 • [常に] (デフォルト): 感染する可能性のあるサイトにアクセスしようとしたときに、警告を表示します。 	
[カーネルキーストロークログをブロックする]	<p>ブラウザに入力されるキーストロークをすべて暗号化して、オペレーティングシステムに潜んでいる悪意のあるソフトウェアコンポーネント(カーネルキーストロークログと呼ばれる)からキーストロークを隠します。</p> <p>これは、[キーロギングをブロックする]を強力にしたものです。カーネルキーストロークログのブロックが有効な場合、Rapportはシステムのカーネルレベルでキーストロークを暗号化します。これにより、キーボードからブラウザまでの経路のあらゆる箇所、キーロガーによるキーストロークの読み取りを不可能にします。</p> <p>[キーロギングをブロックする]が無効な場合、[カーネルキーストロークログをブロックする]は、[常に]に設定されていたとしても無効になります。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。

コントロール	説明	ポリシーオプション	追加情報
	<p>す。[カーネルキーストロークログをブロックする]は、[キーロギングをブロックする]を補完し、強化するものですが、単独で動作することはできません。</p> <p>この機能は、悪意のあるソフトウェアコンポーネントによりキーストロークが読み取られ、クレジットカード番号などの機密情報が詐取されないよう防止することを目的としています。</p>		
[ブラウザ内の許可されないモジュールをブロックする]	<p>ブラウザにロードされたDLLファイルを監視し、ブラウザに悪意のあるファイルが読み込まれないよう防止します。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>この保護はブラウザの起動時に作動するため、パートナーWebサイトと手動で追加したWebサイトを区別せず、すべてのWebサイトを保護します。</p>
[悪意のあるサイトをブラウザしたときに警告を出す]	<p>悪意のあるWebサイトであることが分かっているWebサイトにアクセスした場合、ユーザーに警告します。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>[未知のWebサイトでログイン情報が使用された場合に警告を出す]をクリックすることで、個別のWebサイトのパスワードおよびユーザー名保護ポリシーを確認できます。</p> <p>特定のWebサイトでパスワードまたはユーザー名の保護を無効にする場合は、チェックボックスをオフにすれば、その後未知のWebサイトでパスワードまたはユーザーIDを入力しても、Trusteer Rapportの警告が表示されることは無くなります。</p> <p>保護されたPIIのキャッシュは、クリア</p>

コントロール	説明	ポリシーオプション	追加情報
			<p>できます。キャッシュをクリアした後は、Trusteer Rapportは一切パスワードを保護していない状態になります。また、この操作により、すべての個別の保護されたWebサイトに対するパスワード保護の設定もリセットされます。キャッシュをクリアした後、最初に保護されたWebサイトにログインしたときに、Trusteer Rapportから再度パスワードを保護するかどうかを尋ねられます。キャッシュをクリアするには、まず[未知のWebサイトでログイン情報が使用された場合に警告を出す]をクリックしてから、[キャッシュをクリアする]をクリックします。</p>
<p>[ブラウザのプロセス変更をブロックする]</p>	<p>ブラウザのプロセスを変更しようとする試行をブロックします。ブラウザプロセスの変更(ファンクションパッチとも呼ばれる)は、ブラウザを乗っ取り、機密情報へのアクセスを可能にする手法です。この手法はマルウェアによって使用されますが、一部の正規ソフトウェアでも使用されています。Trusteer Rapportは、各プロセスを変更しようとする試みを解析し、疑わしいものはブロックします。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>この保護はブラウザの起動時に作動するため、パートナーWebサイトと手動で追加したWebサイトを区別せず、すべてのWebサイトを保護します。</p>
<p>[許可されない削除から Rapport を保護する]</p>	<p>Trusteer Rapport自身を、許可されていない削除や変更から保護します。Trusteer Rapportは、プロセスの終了、ファイルの削除や変更、レジストリ</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。Trusteer Rapportはコントロールパネルからしか削除できません(「Trusteer Rapport のアンインストール」(249ページ)を参照)。</p>

コントロール	説明	ポリシーオプション	追加情報
	<p>キーの削除や変更から、Trusteer Rapport自身を保護しています。その結果、Trusteer Rapportではプロセスの終了やファイルの削除などの簡単な操作を行うことができません。Trusteer Rapportでは、マルウェアによりTrusteer Rapport自体が削除されないよう防止するために、このような保護を実施しています。</p>		
[早期ブラウザ保護]	<p>ブラウザの保護を、ブラウザ起動プロセスの可能な限り早い段階で開始します。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>この保護はブラウザの起動時に作動するため、パートナーWebサイトと手動で追加したWebサイトを区別せず、すべてのWebサイトを保護します。</p> <p>Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。</p>
[セキュリティイベントとエラーを解析のために送信する]	<p>Trusteer Rapportが疑わしいソフトウェアまたはWebサイトアクティビティを検知すると、その都度セキュリティイベントが生成され、Trusteer Rapport センtralサービスに送信されて解析されます。センtralサービスは、徹底したテストを実行して、そのアクティビティが不正であるかどうか特定されず。不正なアクティビティであった場合は、</p>	<ul style="list-style-type: none"> • [重大なイベントのみ] • [常に] (デフォルト) 	<p>Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。</p> <p>Trusteerのプライバシーポリシーおよびユーザー情報に関するTrusteerの実務の詳細については、 http://www.trusteer.com/support/privacy-policyおよび http://www.trusteer.com/support/end-user-license-agreementを参照してください。</p>

コントロール	説明	ポリシーオプション	追加情報
	<p>Trusteer Rapport センtralサービスから Trusteer Rapport に対して、より積極的にその脅威をブロックするように指示されます。セキュリティイベントの他にも、Trusteer Rapport はソフトウェアの内部エラーについての情報も随時送信します。この情報は、Trusteer がソフトウェアの問題を特定し、修復するために役立ちます。ご使用のコンピューターから Trusteer Rapport センtralサービスに送信されるすべての情報は匿名であり、技術的な詳細情報が含まれるだけで、個人情報 は含まれません。</p> <p>この機能を無効にすると、セキュリティ上大きな問題があります。実際にオンラインセキュリティが攻撃された場合、この機能により、攻撃を受けたWebサイトのオーナー(銀行</p> <hr/> <p>または企業など)はアラートを受け取り、ユーザーの機密情報や財産の安全を確保するために先手を打つことができます。</p>		

コントロール	説明	ポリシーオプション	追加情報
[マルウェアを駆除する]	Trusteer Rapportは、特定のタイプのマルウェアをコンピューターから駆除します。これにより、マルウェアがユーザーの機密情報にアクセスすることを防ぐ Trusteer Rapportの機能を補完する、重要なセキュリティレイヤーが追加されます。	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。 注: 一部のTrusteer Rapportのインストールでは、この機能は無効にできません。
[クレジットカードの番号を盗難から保護する]	ユーザーがクレジットカード情報をローカルの安全でないWebサイトに送信すると、警告を表示します。この警告が表示されるダイアログボックスを使用して、送信を止めることができます。Trusteer Rapportにより保護されたサイトまたはVisa、MasterCard、Amexなどのクレジットカードに関連するキーワードが含まれるその他の安全な(HTTPS)サイトにユーザーがクレジットカード番号を入力すると、アンチキーロギングがアクティブになります。これは、キーロギングマルウェアによりクレジットカードの詳細がキャプチャーされないように保護するためのものです。	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。 [以下のサイトを信頼することを選択しました。]の下にリストされているサイトは、 「クレジットカード情報送信検知の警告に対する応答」 (129ページ)のダイアログボックスで、 [信頼済みサイトなので、無視する] をクリックして信頼することを選択したサイトです。 信頼されているサイトから特定のサイトを削除するには、削除するWebサイトの横にある [このサイトをクリアする] をクリックします。すべてのサイトを削除するには、 [すべてのサイトをクリアする] をクリックします。 Trusteer Rapportがアンチキーロギングをアクティブにしたときに、通知を受け取る必要がない場合は、 [Notify me when Trusteer activates payment card protections] チェックボックス(デフォルトでは有効)をオフにします。 クレジットカード情報をローカルおよび安全でないWebサイトに送信するときに警告を受け取る必要がない場合は、 [Rapportにより高リスクのクレジットカード送信が検知されたときにアラートを出す] チェックボックス(デフォルトでは有効)をオフにします。

コントロール	説明	ポリシーオプション	追加情報
	<p>この機能は、マルウェアがユーザーのクレジットカード情報をキャプチャできないようにし、さらにユーザーがクレジットカード番号をフィッシングWebサイトや安全でないWebサイトに送信してしまうことを防止することで、ユーザーをクレジットカード情報盗難から保護することを目的としています。</p> <p>この保護は、登録しているカード会社によって発行されたカードのみで利用可能です。</p>		
[安全ではないサイトにセキュリティデータを送信する場合に警告する]	<p>データを安全に送信しないWebサイトにユーザーがパスワードを入力した場合、ユーザーに警告します。この機能は、リスクの高いサイトへの機密情報の送信を防止することを目的としています。リスクの高いサイトには、犯罪者が簡単に情報をインターセプトできる正規Webサイトも含まれます。</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>Trusteer Rapportを管理者レベルのアカウントからインストールした場合、管理者アカウントでログインしている場合のみ、この設定を変更できます。</p> <p>[以下のサイトを信頼することを選択しました。]の下にリストされているサイトは、「安全でない送信の警告に対する応答」 (119ページ)のダイアログボックスで[信頼済みサイトなので、再警告を出力しない]をクリックするか、保護情報の警告ダイアログボックスで[このサイトを信頼する]をクリックして信頼することを選択したサイトです。</p> <p>信頼されているサイトから特定のサイトを削除するには、削除するWebサイトの横にある[このサイトをクリアする]をクリックします。すべてのサイトを削除するには、[すべてのサイトをクリアする]をクリックします。</p>
[Trusteer Rapportの仮想化ブラウザを対応サイト]	<p>Trusteer Rapportの仮想化ブラウザをサポートしているサイトをブラウザしたときにアラートを表示</p>	<ul style="list-style-type: none"> • [しない] • [常に] (デフォルト) 	<p>「仮想化ブラウザのオプションダウンロードアラートに対する応答」 (95ページ)または「仮想化ブラウザのオプションアラートに対する応答」 (101ページ)のアラートで、[この警告メッ</p>

コントロール	説明	ポリシーオプション	追加情報
<p>で使用することを推奨する]</p>	<p>し、コンピューターに仮想化ブラウザがインストールされている場合は、仮想化ブラウザでサイトを開くことを促します。コンピューターに仮想化ブラウザがインストールされていない場合は、アラートにより仮想化ブラウザのダウンロードが促されま</p>		<p>ページを再出力しない]をクリックした場合は、このポリシーは[しない]に設定されています。ドロップダウンボックスを使用して、ポリシーを[常に]に切り替えると、次回仮想化ブラウザをサポートしているサイトにアクセスしたときに、アラートが表示されます。</p> <p>[以下のサイトに対して、仮想化ブラウザのアラートを表示しないことを選択しました。]の下にリストされているサイトは、サイトに「仮想化ブラウザのオプションダウンロードアラートに対する応答」(95ページ)または「仮想化ブラウザのオプションアラートに対する応答」(101ページ)のアラートが表示されたときに、[このサイトでは再通知しない]をクリックしたサイトです。</p> <p>[仮想化ブラウザを使用して、以下のサイトを開くことを選択しました。]の下にリストされているサイトは、サイトに「仮想化ブラウザのオプションアラートに対する応答」(101ページ)のアラートが表示されたときに、[このサイトを登録する]チェックボックスをオンにしてから[はい]をクリックしたサイトです。</p> <p>上記のいずれかのサイトから特定のサイトを削除するには、削除するWebサイトの横にある[サイトを削除する]をクリックします。すべてのサイトを削除するには、[すべてのサイトをクリアする]をクリックします。</p>

17. トラブルシューティング

Trusteer Rapportで問題が発生した場合は、トラブルシューティングFAQ (<http://www.trusteer.com/support/faq>)をご利用ください。

サポートへの問い合わせ方法については、[「サポートについて」](#) (210ページ)を参照してください。以下の項では、トラブルシューティングが必要な状況で実施するいくつかの手順を説明します。

Trusteer Rapportは、コンピューターから削除しなくても、随時停止できます ([「Trusteer Rapportの停止」](#) (207ページ)を参照)。これにより、特定の問題がTrusteer Rapportに関連しているかどうかを確認できます。トラブルシューティング中に、Trusteer Rapportを削除することは、できる限り避けてください。[「Trusteer Rapportの停止」](#) (207ページ)でも削除と同じ効果があり、ユーザーがサポートに問い合わせたときに、Trusteerが素早く効果的に問題を解決することができます。

Trusteer Rapportの停止

Rapportを停止すると、アンインストールしなくても、Trusteer Rapportの機能を素早く簡単にシャットダウンできます。Rapportを停止することで、問題の原因がTrusteer Rapportで発生しているかどうかを特定できます。Trusteer Rapportを再度実行する場合は、再インストールは必要なく、[「Trusteer Rapportの起動」](#) (209)を実行するだけで済みます。

Trusteer Rapportが原因である可能性がある問題が発生した場合は、Rapportの停止をお試しください。Trusteer Rapportを停止した後も問題が続く場合は、Trusteer Rapportがその問題の原因であるとは考えにくいです。Rapportを停止したとことで問題が解決した場合は、その問題の少なくとも一部の原因になっている可能性が高いと思われます。

Trusteerでは、Trusteer Rapportのアンインストールは推奨しません。Trusteer Rapportのアンインストールを検討されている場合は、[「サポートについて」](#) (210ページ)を参照して、一度サポートにお問い合わせください。

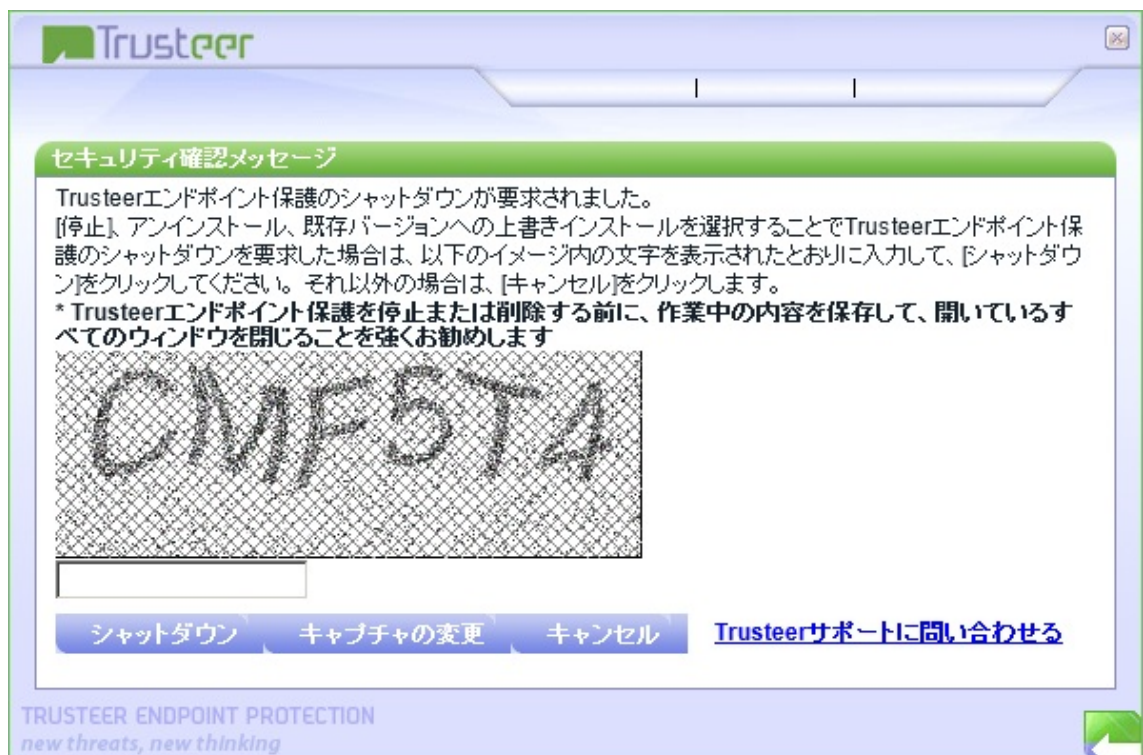
Trusteer RapportをWindowsの管理者アカウントからインストールした場合、管理者アカウントにログインしている場合のみ、Trusteer Rapportを停止できません。

➔ Trusteer Rapportの停止方法

1. 作業を保存し、開いているウィンドウをすべて閉じます。

注: ブラウザーを開いているときに、Trusteer Rapportを停止しないでください。ブラウザーを開いているときにTrusteer Rapportを停止すると、故障するおそれがあります。

2. Windowsのスタートメニューから、[すべてのプログラム] > [Trusteer Rapport] > [Rapportを停止する]を選択します。セキュリティ確認メッセージが表示されます。このメッセージには、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアによりTrusteer Rapportが無効化されることを防止するためのものです。



3. 画像に表示された文字を入力します。


4. [シャットダウン]をクリックします。Trusteer Rapportのシャットダウン中に、[Rapportがシャットダウンするまでお待ちください...]というメッセージが表示されます。Trusteer Rapportが動作を停止すると、メッセージが消えます。ブラウザを開き、アドレスバーの右端にTrusteer Rapportアイコンが表示されないことを確認することで、Trusteer Rapportが実行されていないことを確認できます。

Trusteer Rapportの起動

Trusteer Rapportを停止した場合、Rapportを起動することで再開できます。

注: Trusteer RapportをWindowsの管理者アカウントからインストールした場合、管理者アカウントにログインしている場合のみ、Trusteer Rapportを起動できます。

➔ Trusteer Rapportの起動方法

Windowsのスタートメニューから、[すべてのプログラム] > [Trusteer Trusteer Rapport] > [スタート]を選択します。[Rapportが起動するまでお待ちください...]というメッセージが表示されます。Trusteer Rapportが再起動すると、メッセージが消えます。システムトレイにRapportアイコンがあることを確認することで、Trusteer Rapportが実行されていることを確認できます()。

サポートについて

Trusteerのサポートは、24時間対応で年中無休です。Trusteerでは、いくつかのサポートオプションを提供しています。


- コンピューターにTrusteer Rapportがインストールされており、接続に問題が無い場合は、Rapportコンソールから問題のレポートを開始できます。「[ユーザー問題レポートの送信](#)」(234ページ)を参照してください。Rapportコンソールから問題をレポートすると、Trusteer RapportからTrusteerに、サポートリクエストと問題レポート、およびTrusteerが問題を解決するうえで役立つ重要なログファイルが送信されます。
- Trusteer Rapportがインストールされておらず、Trusteer Rapport経由でサポートリクエストを送信できない場合は、所定のフォーム(<http://www.trusteer.com/support/submit-ticket>)を使用してサポートリクエストを送信してください。その際、問題およびご使用のコンピューターの両方について、できるだけ多くの情報(使用しているオペレーティングシステム、使用しているブラウザ、発生している動作など)を記載してください。
- パフォーマンス、接続性、安定性、またはブラウザの機能に問題がある場合は、[ライブサポート]リンク(<http://www.trusteer.com/support>)をクリックして、サポート担当者とのオンラインチャットを開始してください。

注: 問題は発生していないが、Trusteer Rapportについて不明点がある場合は、本書を検索していただくか、Webページ(<http://www.trusteer.com/support/faq>)でnanoRepサービスを使用してください。

正規ブラウザアドオンのブロック解除

ブラウザで特定のWebページを正確に表示できず、正規のアドオンがブロックされている可能性が疑われる場合は、Trusteer Rapportがそのアドオンをブロックしているかを確認できます。

➔ 正規ブラウザーアドオンのブロック解除方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。

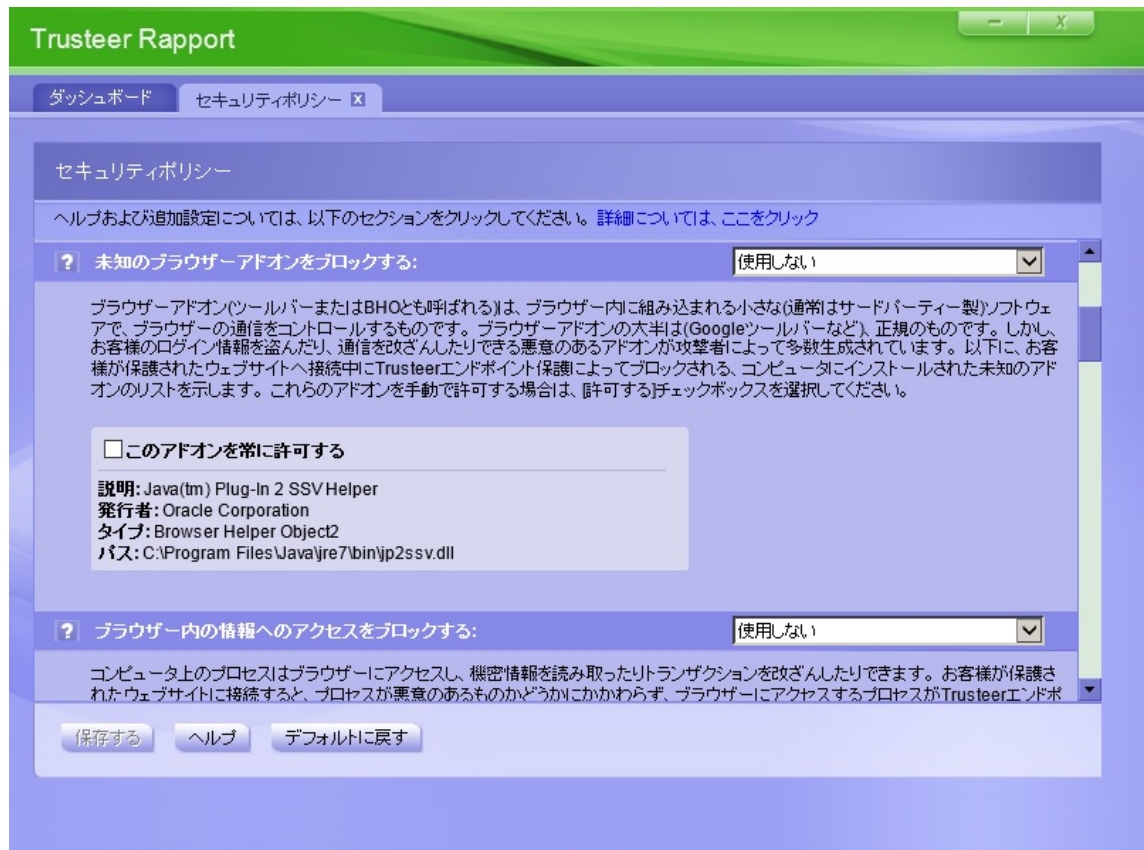


3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。



6. [未知のブラウザアドオンをブロックする]をクリックします。ブロックされたアドオンの一覧が表示されます。ブロックされた各アドオンの横には、[このアドオンを常に許可する]チェックボックスがあります。




7. ブロックされているアドオンのうち、許可したいものの横にある[このアドオンを常に許可する]チェックボックスをオンにします。
8. [保存する]をクリックします。当該のアドオンのブロックが解除されました。

キーロガーブロック機能の無効化

Trusteer Rapportのキーロガーブロック機能は、その他のアンチキーロガーと機能衝突し、キーストロークがスクランブル化される場合があります。そのため、別のキーロガーを実行している場合(ご使用のアンチウイルスソフトウェアに組み込まれている場合など)は、この機能を無効にする必要があります。または、既存のソフトウェアのキーロギング保護を無効にすることもできます。

➔ キーロガーブロック機能の無効化方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。

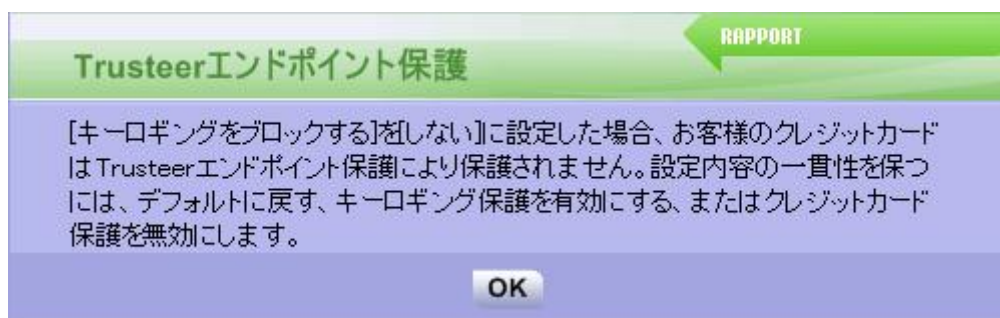


3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
ここには、すべてのセキュリティコントロールが表示されています。



6. [キーロギングをブロックする]の横にあるドロップダウンリストで、[しない]を選択します。以下のメッセージが表示されます。



7. [OK]をクリックします。
8. [カーネルキーストロークログをブロックする]の横にあるドロップダウンリストで、[しない]を選択します。
9. [保存する]をクリックします。変更はコンピューターを再起動した後に有効になることを知らせるメッセージが表示されます。

10. [OK]をクリックします。

11. コンピューターを再起動します。Trusteer Rapportのキーロガーブロック機能が無効になりました。

誤った承認の取り消し


Trusteer Rapportの警告の中には、Trusteer Rapportが正規のものであると認識していないWebサイトまたは証明書を承認できるものがあります。いったんWebサイトまたは証明書を承認すると、そのWebサイトまたは証明書はキャッシュに保存され、以降これに関する警告は表示されなくなります。誤ってWebサイトまたは証明書を承認してしまった場合は、キャッシュをクリアして、対象のサイトに再度接続した際に、同じWebサイトまたは証明書に対する警告が表示されるようになります。

承認された無効なSSL証明書のクリア

Webサイトの[証明書](#)⁶が無効であることを検知した場合、Trusteer Rapportは、無効な証明書の警告([「無効な証明書の警告への応答」](#) (141ページ)参照)を表示して、不正なWebサイトに情報を送信しないよう防止します。無効な証明書の警告ダイアログボックスで、**[このサイトで再警告を出力しない]**チェックボックスをオンにした場合、接続使用としているWebサイトの証明書が、承認された無効な証明書のキャッシュに追加されます。そのキャッシュをクリアすると、キャッシュ内のすべての証明書の承認が削除され、同じWebサイトを再度ブラウズしたときに、Trusteer Rapportから再度警告が表示されるようになります。

⁶ SSL証明書は、暗号化されたデジタル証明書で、WebサイトのIDを検証し、Webサイトに機密の個人データを送信するための暗号化された接続を確立します。ブラウザーのアドレスバーまたはブラウザーの下部にSSLの南京錠が表示された場合は、SSLプロトコルを使用して、ブラウザーとWebサイト間の安全な接続が確立されていることを意味します。ただし、これは証明書が有効であることを通知するものではありません。

➔ 承認された無効なSSL証明書のクリア方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここでは、すべてのセキュリティコントロールが表示されています。




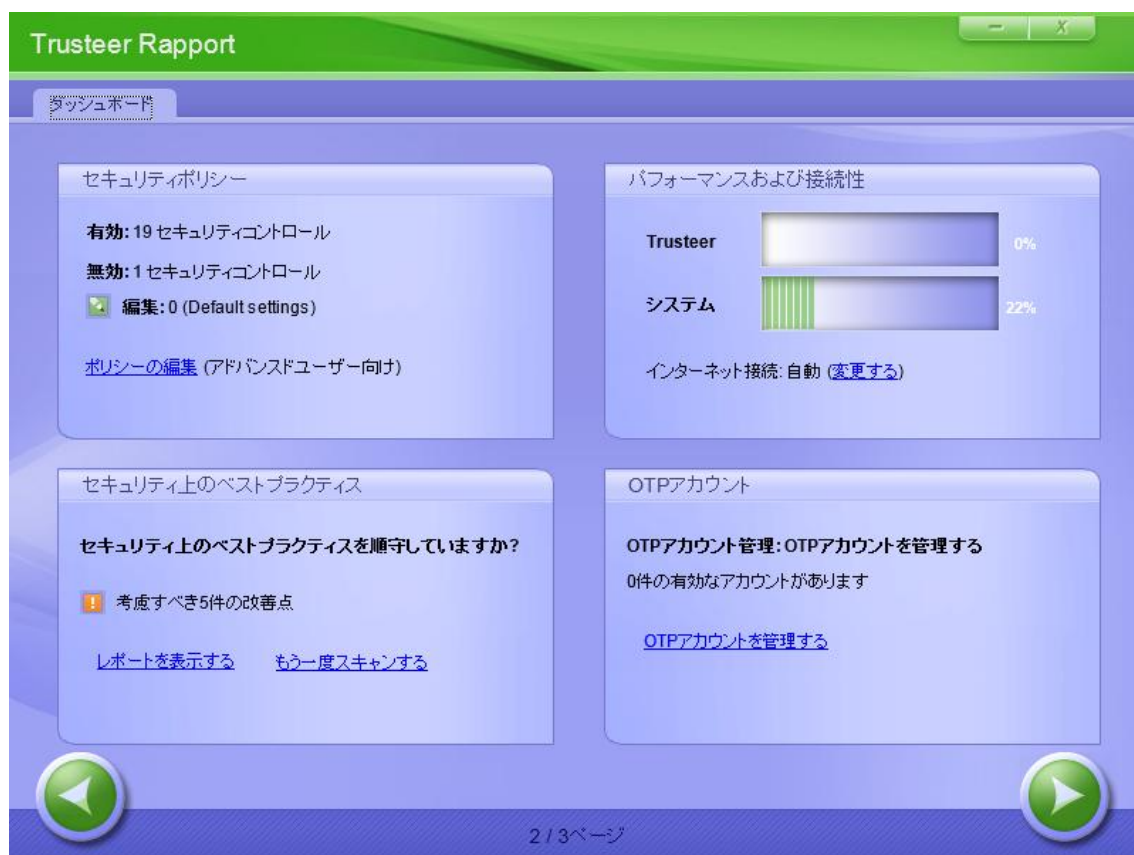
6. **[WebサイトのSSL証明書を検証する]**をクリックします。このコントロールについての情報と、**[キャッシュをクリアする]**ボタンがその下に表示されます。
7. 拡張情報ブロックで、**[キャッシュをクリアする]**をクリックします。確認ボックスが表示されます。
8. **[OK]**をクリックします。キャッシュがクリアされます。

クレジットカード情報送信用の信頼済みサイトのクリア

ローカルドライブまたは安全でないWebサイトに存在するWebページに、保護されたクレジットカード番号を入力したことを検知した場合、Trusteer Rapportは、クレジットカード情報送信検知の警告([「クレジットカード情報送信検知の警告に対する応答」](#) (129ページ)を参照)を表示します。このメッセージボックスは、フィッシングWebサイトまたは安全でない正規のWebサイトへの、クレジットカード番号の送信を回避することを目的としています。クレジットカード情報送信検知の警告ダイアログボックスで[信頼済みサイトなので、無視する]をクリックした場合、このWebサイトはユーザーが信頼すると選択したWebサイトのリストに追加され、今後このサイトにクレジットカード番号を入力しても、警告が表示されることは無くなります。リストから、サイトを削除することもできます。

➔ クレジットカード情報送信信用の信頼済みサイトのクリア方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
 ここには、すべてのセキュリティコントロールが表示されています。




6. **[クレジットカードの番号を盗難から保護する]**というコントロールをクリックします。拡張領域に、信頼すると選択したすべてのサイトが一覧表示されます。これらは、クレジットカード情報送信検知の警告ダイアログボックスで、ユーザーが**[信頼済みサイトなので、無視する]**をクリックして信頼すると選択したサイトです。
7. **[このサイトをクリアする]**ボタンをクリックしてリストから個々にサイトを削除するか、**[すべてのサイトをクリアする]**ボタンをクリックして、すべての信頼済みサイトを削除します。確認ボックスが表示されます。
8. **[OK]**をクリックします。

安全でない送信警告用の信頼済みサイトのクリア

データを安全に送信しないWebサイトにパスワードを入力したことを検知した場合、Trusteer Rapportは、安全でない送信の警告([「安全でない送信の警告に対する応答」](#) (119ページ)を参照)を表示します。この警告の目的は、リスクの高いサイトへの機密情報の送信を防止するものです。リスクの高いサイトには、犯罪者が簡単に情報をインターセプトできる正規Webサイトも含まれます。

[「安全でない送信の警告に対する応答」](#) (119ページ)のダイアログボックスで **[信頼済みサイトなので、再警告を出力しない]** をクリックした場合、このWebサイトはユーザーが信頼すると選択したWebサイトのリストに追加され、今後このサイトにクレジットカード番号を入力しても、警告が表示されることはなくなります。リストから、サイトを削除することもできます。

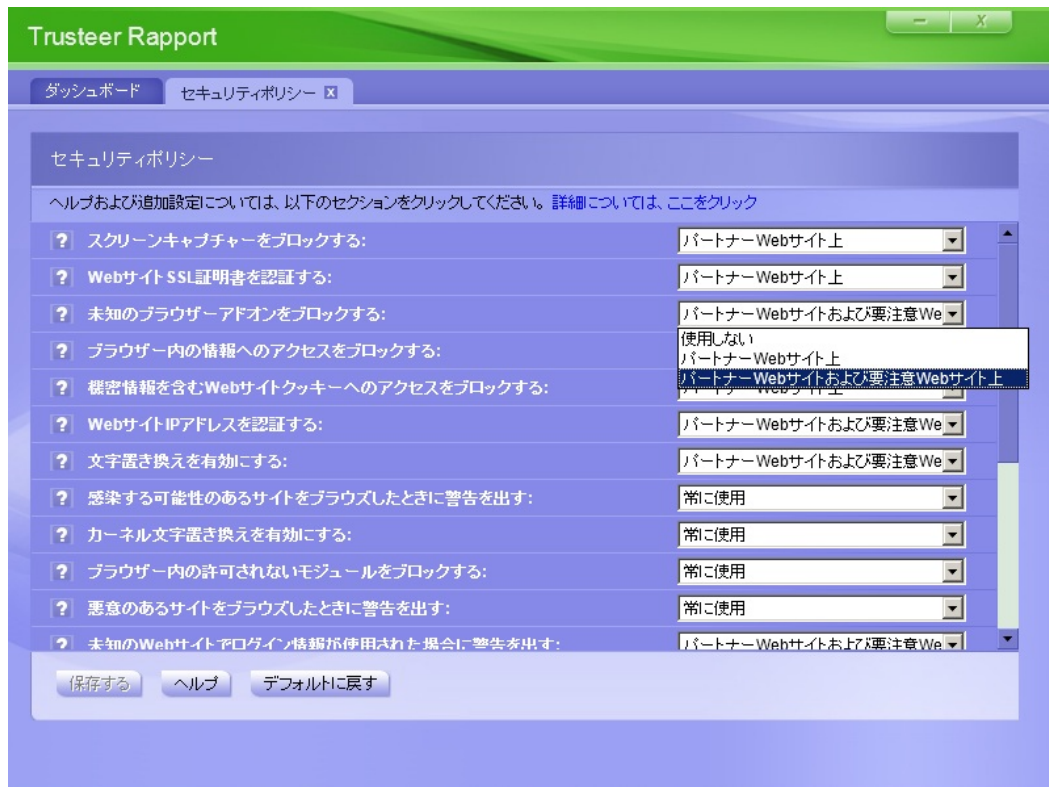
➔ 信頼すると選択した安全でないWebサイトのクリア方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. [OK]をクリックします。[セキュリティポリシー]画面が表示されます。
ここには、すべてのセキュリティコントロールが表示されています。




6. [安全ではないサイトにセキュリティデータを送信する場合に警告する]
というコントロールをクリックします。拡張領域に、信頼すると選択し
たすべてのサイトが一覧表示されます。これらは、[「安全でない送信の
警告に対する応答」](#) (119ページ)のダイアログボックスで[信頼済みサイ
トなので、再警告を出力しない]をクリックするか、保護情報の警告ダイ
アログボックスで[このサイトを信頼する]をクリックして信頼するこ
とを選択したサイトです。
7. [このサイトをクリアする]ボタンをクリックしてリストから個々にサイ
トを削除するか、[すべてのサイトをクリアする]ボタンをクリックして、
すべての信頼済みサイトを削除します。確認ボックスが表示されます。
8. [OK]をクリックします。

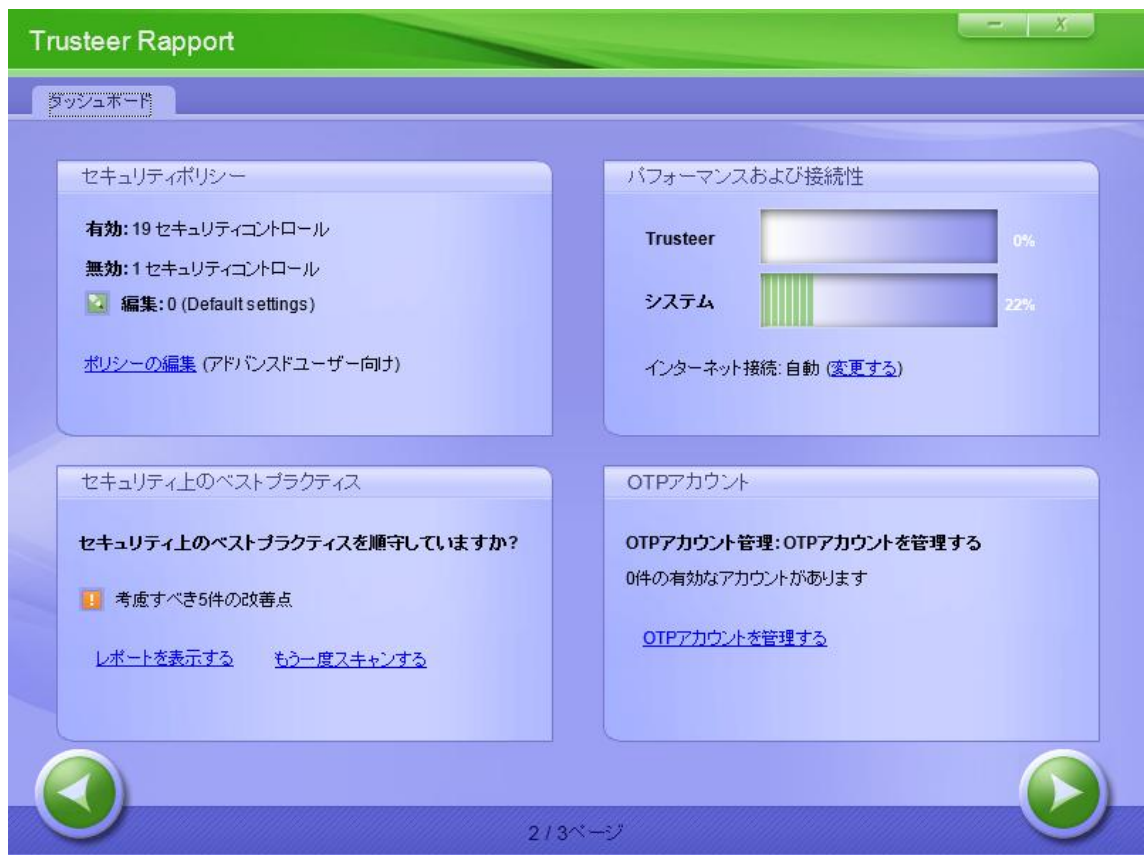
ログイン情報の送信先として許可したWebサイトのクリア

不明なWebサイトに保護されたパスワードに一致するテキストを入力した場合、Trusteer Rapportは、保護情報の警告([「保護情報の警告に対する応答」](#) (117 ページ)を参照)を表示します。警告を無視することを選択した場合、Webサイトが承認されたWebサイトになり、そのWebサイトに保護されたパスワードを入力しても、Trusteer Rapportから警告が表示されることは無くなります。この方法で承認したWebサイトは、キャッシュに保存されます。そのキャッシュをクリアすると、同様の承認がすべて削除されます。

保護情報の警告ダイアログボックスで誤って[警告メッセージを無視する]をクリックした場合は、ログイン情報の送信を許可した、承認済みWebサイトのキャッシュをクリアします。この操作は、すでに実行したパスワード送信を取り消すものではなく、誤って承認してしまった可能性のある、不明なWebサイトの状態をリセットするものです。

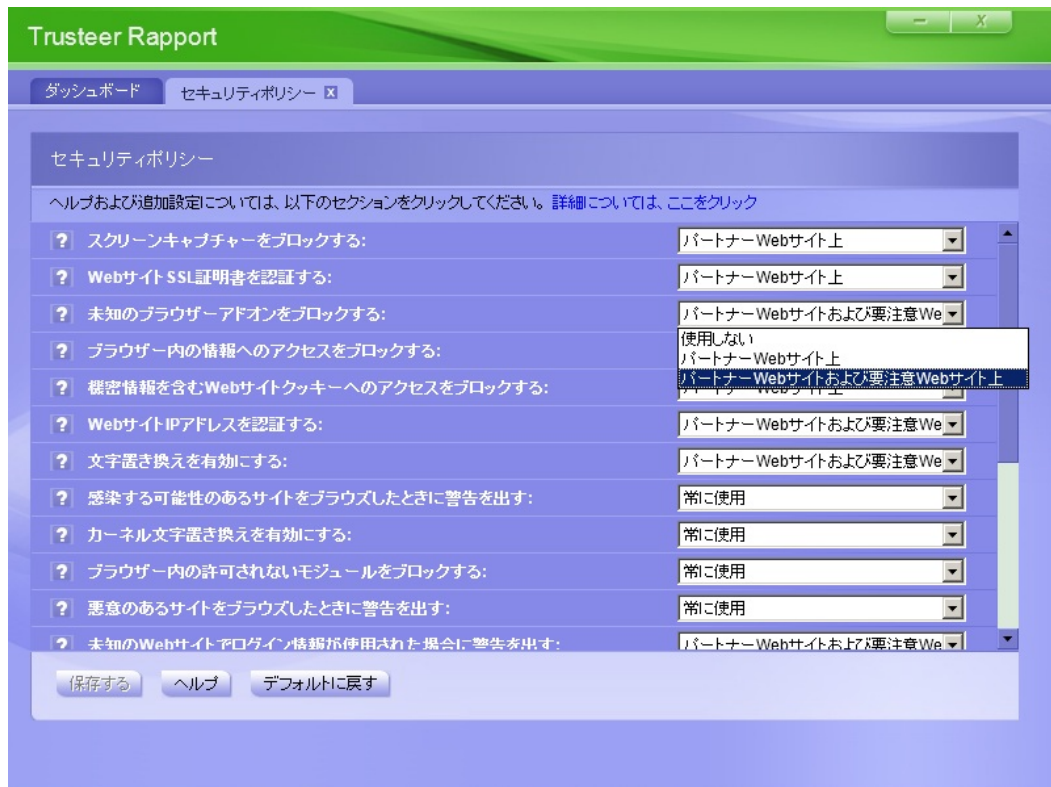
➔ ログイン情報の送信を許可した承認済みWebサイトのキャッシュのクリア方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。
2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



3. [セキュリティポリシー]領域で、[ポリシーの編集]をクリックします。
[ユーザーによる許可]画面が開きます。この画面には、ユーザーが入力する文字が示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。
4. 画像に表示された文字を入力します。

5. **[OK]**をクリックします。**[セキュリティポリシー]**画面が表示されます。
ここでは、すべてのセキュリティコントロールが表示されています。



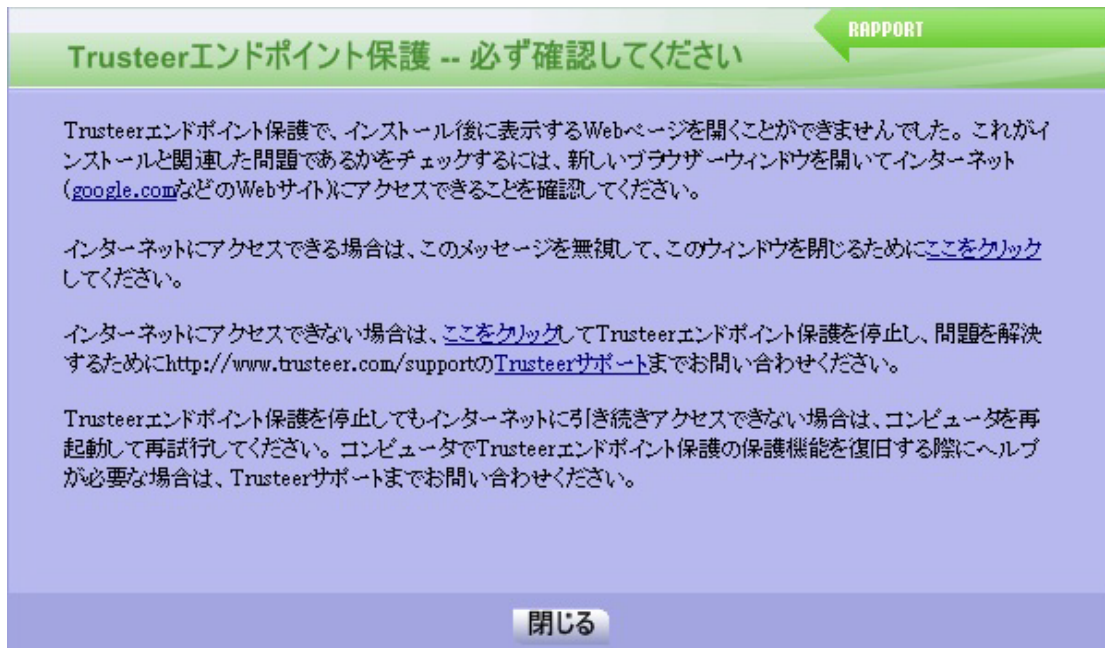
6. **[未知のWebサイトでログイン情報が使用された場合に警告を出す]**までスクロールし、このコントロール名をクリックします。このコントロールについての情報と、**[キャッシュをクリアする]**ボタンがその下に表示されます。
7. 拡張情報ブロックで、**[キャッシュをクリアする]**をクリックします。確認ボックスが表示されます。
8. **[OK]**をクリックします。キャッシュがクリアされます。

エラーへの対応

Trusteer Rapportのエラーが表示され、そのエラーに関する情報を確認したい場合は、本項を読んでください。

ポストインストールWebページエラーへの対応

以下に、ポストインストールWebページエラーの例を示します。

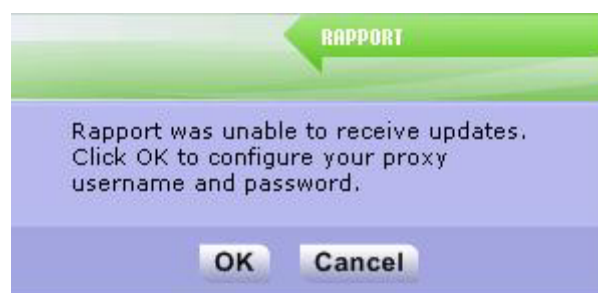


このエラーは、Trusteer Rapportをインストールした後に、Trusteer Rapportがユーザーのデフォルトブラウザを起動して、短い互換性テストを実行できなかった場合に表示されます。

このアラートが表示されたら、インターネットブラウザを使用して、オンラインに接続できるかどうかを確認します。その後、ダイアログボックスの指示に従ってください。

更新エラーへの対応

以下に、Trusteer Rapportの更新エラーの例を示します。



このエラーは、Trusteer Rapportがインターネットに接続して、更新の有無を確認できなかった場合に表示されます。このエラーの原因は、ユーザーがインターネットにプロキシを経由して接続しているため、Trusteer Rapportがそのプロキシの詳細を自動的に検知できなかったことにあります。このダイアログボックスを使用して、Trusteer Rapportがインターネットに接続して更新を取得できるように、プロキシサーバーを設定できます。

➔ このエラーへの対応方法

1. [OK]をクリックします。Rapportコンソールが開き、[インターネット接続]タブが表示されます。

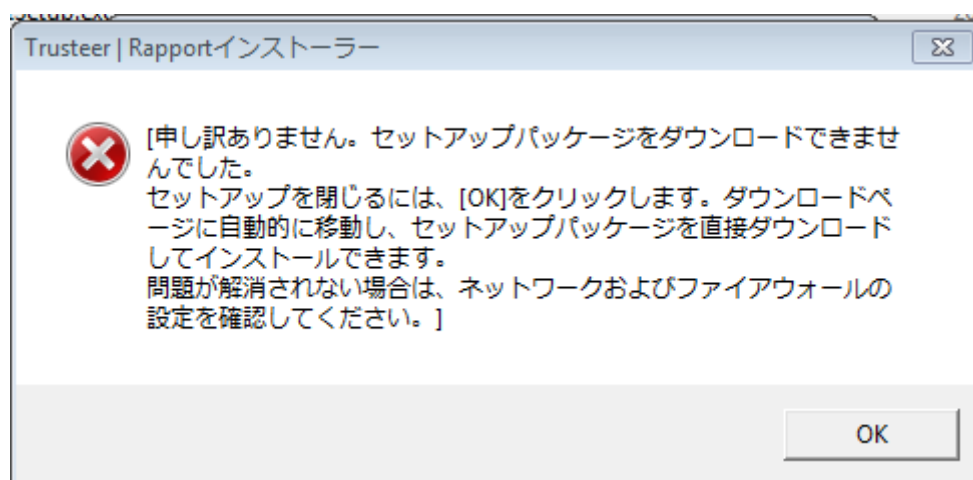


2. [プロキシサーバーを使用する]を選択します。表示されるフィールドに、プロキシサーバー名またはIPアドレスを入力します。
3. [ポート]フィールドに、プロキシサーバーに接続するために使用しているTCPポートを入力します。

4. プロキシサーバーで認証を要求している場合は、[プロキシユーザー名]フィールドにユーザー名を、[プロキシパスワード]フィールドにパスワードを入力します。
5. [設定を適用する]をクリックします。
6. [接続をチェックする]をクリックして、プロキシサーバーを設定したことにより、Trusteer Rapportがインターネットに接続できるようになったことを確認します。

Rapportインストーラーエラー

以下に、Trusteer Rapportインストーラーエラーの例を示します。



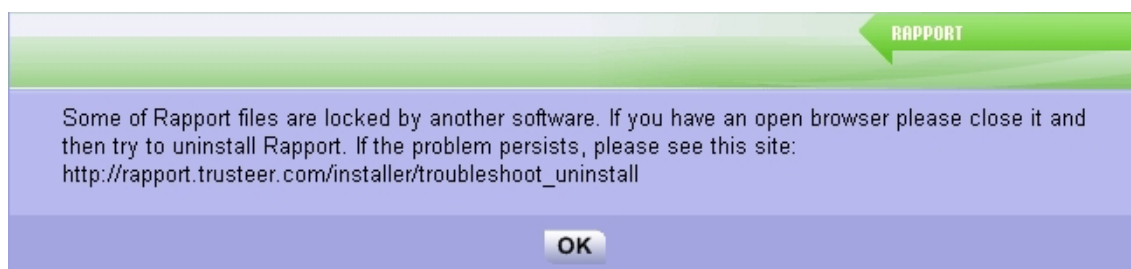
このエラーは、Trusteer Rapportのインストール中に、Rapportインストーラーが設定パッケージを完全にダウンロードできなかった場合に表示されます。

このエラーが表示されたら、[OK]をクリックしてください。TrusteerのWebサイトが開きます。TrusteerのWebサイトから、すべての設定パッケージを直接ダウンロードします。

注: Webサイトの説明では不明な場合は、Trusteerサポート (<http://www.trusteer.com/support/submit-ticket>) にお問い合わせください。

アンインストールエラーへの対応

以下に、アンインストールプロセス中に発生する可能性のあるエラーの例を示します。



このダイアログボックスは、Trusteer Rapportをアンインストールしようとしたときに、別のプログラムによりTrusteer Rapportのいずれかのファイルがロックされている場合に表示されます。

このエラーが表示されたら、ダイアログボックスの指示に従ってください。ダイアログボックスに引用されているWebサイトで、安全なアンインストールユーティリティをダウンロードできます。このユーティリティを使用して、Trusteer Rapportをアンインストールできます。


注: Webサイトの説明では不明な場合は、Trusteer サポート (<http://www.trusteer.com/support/submit-ticket>) にリクエストを送信してください。

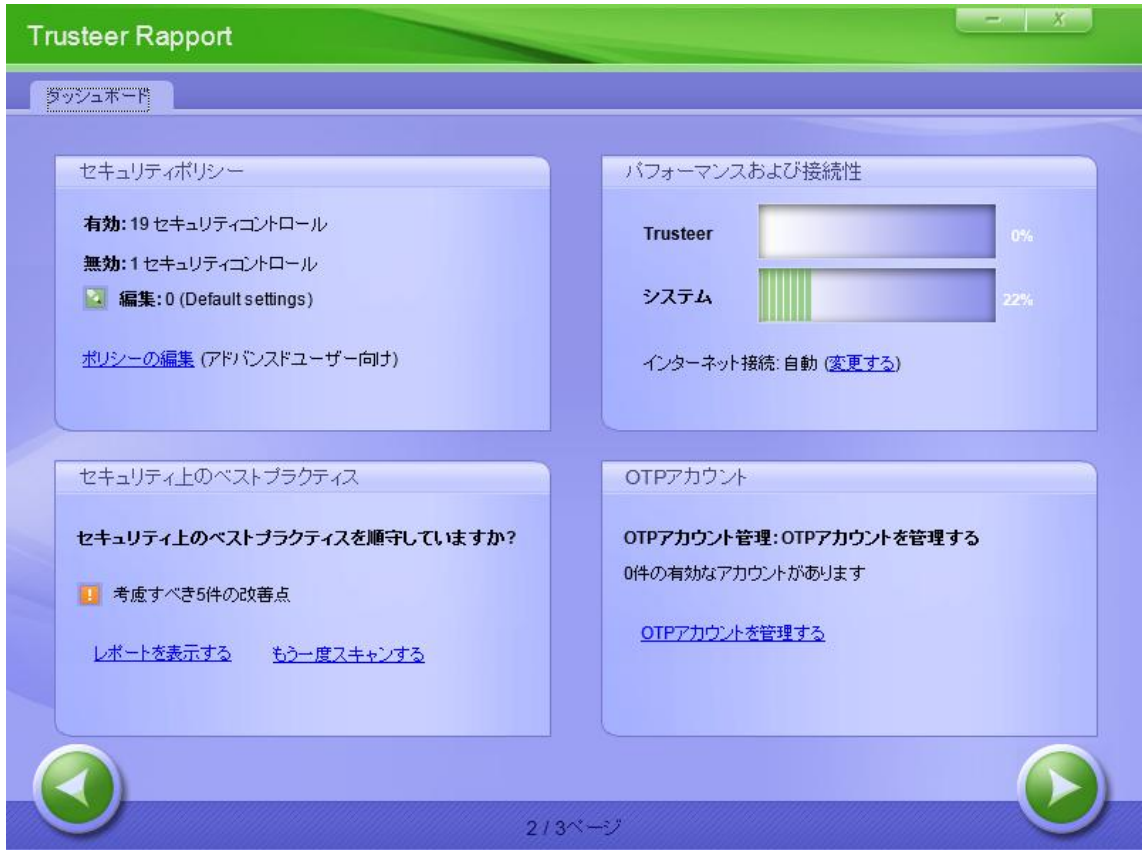
プロキシサーバーの自動更新の設定

Trusteer Rapportは、自動的にインターネットに接続して更新の有無を確認し、セキュリティポリシーをダウンロードします。何も設定しなくても、ほとんどのプロキシ設定はTrusteer Rapportにより自動的に検知されます。ただし、何らかの理由でTrusteer Rapportが自動的にプロキシを検知できない場合は、設定が必要になります。

➔ プロキシサーバーの設定方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。

2. ダッシュボードで、をクリックします。画面に2つ目のダッシュボード画面が表示されます。



The screenshot displays the Trusteer Rapport dashboard with the following sections:

- セキュリティポリシー (Security Policies):** Shows 19 active and 1 inactive security controls. Includes a link to edit policies for advanced users.
- パフォーマンスおよび接続性 (Performance and Connectivity):** Displays progress bars for Trusteer (0%) and System (22%). Includes a link to change internet connection settings.
- セキュリティ上のベストプラクティス (Security Best Practices):** Asks if best practices are followed, highlighting 5 areas for improvement. Includes links to view reports and rescan.
- OTPアカウント (OTP Accounts):** Shows 0 active accounts and a link to manage them.

Navigation arrows and page number (2 / 3 ページ) are visible at the bottom.

3. [パフォーマンスおよび接続性]領域の[インターネット接続]フィールドの横にある、[変更する]をクリックします。[インターネット接続]タブが表示されます。

Trusteer Rapport

ダッシュボード インターネット接続

インターネット接続

Trusteerエンドポイント保護は、インターネットに接続して更新の有無をチェックします。
インターネット接続を設定する:

自動的にプロキシを検知する (推奨)
 インターネットへの直接接続
 プロキシサーバーを使用する: ポート:

お客様のインターネット接続環境で認証が必要な場合は、以下の情報を入力してください。

プロキシユーザー名:
 プロキシパスワード:

設定を更新済み

4. [プロキシサーバーを使用する]を選択します。表示されるフィールドに、プロキシサーバー名またはIPアドレスを入力します。
5. [ポート]フィールドに、プロキシサーバーに接続するために使用しているTCPポートを入力します。
6. プロキシサーバーで認証を要求している場合は、[プロキシユーザー名]フィールドにユーザー名を、[プロキシパスワード]フィールドにパスワードを入力します。
7. [設定を適用する]をクリックします。
8. [接続をチェックする]をクリックして、プロキシサーバーを設定したことにより、Trusteer Rapportがインターネットに接続できるようになったことを確認します。

ユーザー問題レポートの送信

Trusteer Rapportの問題レポート機能を使用すると、Trusteer Rapportにより、テクニカルレポートと、重要なTrusteer Rapportの内部ログファイル、および問題の説明が送信されます。このテクニカルレポートは、Trusteerが問題を特定し、解決する際に役立ちます。この方法で問題をレポートすると、問題についての非常に包括的な情報がTrusteerに渡され、Trusteerが最適なサポートを提供するために役立つため、問題のレポート方法としてはこの方法が最適です。

注: ログファイル内の情報は、技術的なものであり、ユーザーの機密情報や個人情報を含みません。

➔ 問題のレポート方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。ダッシュボードが表示されます。



2. [ヘルプとサポート]領域で、[問題をレポートする]をクリックします。
[問題をレポートする]タブが表示されます。

Trusteer Rapport

ダッシュボード 問題をレポートする

問題をレポートする

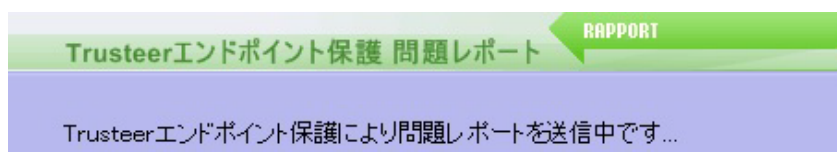
発生した問題の状況を記載して、[送信する]をクリックしてください。
Trusteerエンドポイント保護は、このフォームとともに、内部ログファイルを自動的に送信します。これは発生した問題を解析する上で役立ちます。ログファイルを送信しない場合またはこのフォームを使用できない場合は、以下の窓口まで直接お問い合わせください。 support@trusteer.com

名前(省略可能):

メール:

問題の説明:

3. 任意で、[名前]フィールドにユーザーの名前を入力します。
4. [電子メール]フィールドに、ユーザーの電子メールアドレスを入力します。Trusteerは、このアドレスに問題の解決策を送信します。
5. [問題の説明]フィールドに、問題の説明を詳しく入力します。できるだけ多くの詳細を含めてください。
6. [送信する]をクリックします。Trusteer Rapportが問題のレポートを送信している間、画面の右下に以下のメッセージが表示されます。



レポートが送信されると、レポートが送信されたことを確認するメッセージが表示されます。



Trusteerの担当者から電子メールで問題のサポートについて連絡があります。

TrusteerへのTrusteer Rapportログファイルの送信

Trusteerのサポートから、問題の解決に役立てるために、ご使用のコンピューター上でTrusteer Rapportログファイルを見つけてTrusteerに送信するように依頼された場合は、以下の手順を実行します。

- [「Windows 7でのログの収集」](#) (236ページ)
- [「Windows XPでのログの収集」](#) (238ページ)

Windows 7でのログの収集

➔ Windows 7コンピューターでのRapportログファイルの収集方法

1. Windowsの[スタート]メニューから、[ファイル名を指定して実行]をクリックします。[ファイル名を指定して実行]コマンドウィンドウが開きます。
2. [ファイル名を指定して実行]コマンドウィンドウで、
`%appdata%\trusteer\rapport\user\logs`と入力します。
3. [OK]をクリックします。フォルダーが開き、Trusteer Rapportに関連するログファイルのリストが表示されます。
4. [整理]メニューで、[すべて選択]を選択します。フォルダー内のすべてのファイルが選択されます。

5. マウスを右クリックし、右クリックメニューから[コピー]を選択します。
6. ログファイル用のフォルダーを作成します。たとえば、以下のような手順を実行します。
 - a. デスクトップでマウスを右クリックして[新規作成]をクリックし、[フォルダー]を選択します。
 - b. フォルダーに**Logs**という名前を付けます。
7. ログファイル用として作成したフォルダーを開きます。フォルダーアイコンをダブルクリックすれば開きます。
8. 開いたログファイル用のフォルダー内でマウスを右クリックし、右クリックメニューから[貼り付け]を選択します。コピーしたすべてのファイルが、フォルダーに貼り付けられます。
9. Windowsの[スタート]メニューから、再度[ファイル名を指定して実行]をクリックします。再度[ファイル名を指定して実行]コマンドウィンドウが開きます。
10. [ファイル名を指定して実行]コマンドウィンドウで、
`%programdata%\Trusteer\Rapport\user\logs`と入力します。
11. [OK]をクリックします。フォルダーが開き、Trusteer Rapportに関連する別のログファイルのリストが表示されます。
12. [整理]メニューで、[すべて選択]を選択します。フォルダー内のすべてのファイルが選択されます。
13. マウスを右クリックし、右クリックメニューから[コピー]を選択します。
14. 作成したログファイル用のフォルダーに戻ります。
15. ログファイル用のフォルダー内でマウスをクリックして、先程貼り付けたすべてのファイルが選択されていないことを確認します。

- 16.開いたログファイル用のフォルダー内でマウスを右クリックし、右クリックメニューから**[貼り付け]**を選択します。2番目にコピーしたログファイルのセットが、フォルダーに貼り付けられます。
- 17.ログファイル用のフォルダーを閉じます。
- 18.ログファイル用のフォルダー(デスクトップ上または内部にこのフォルダーを作成したフォルダー内)を右クリックして**[送る]**をクリックし、**[圧縮(zip形式)フォルダー]**を選択します。zip形式に圧縮されたログファイル用のフォルダーが作成されます。
- 19.圧縮されたフォルダーを、電子メールで**support@trusteer.com**に送信します。

Windows XPでのログの収集

➔ Windows XPコンピューターでのRapportログファイルの収集方法

1. Windowsの**[スタート]**メニューから、**[ファイル名を指定して実行]**をクリックします。**[ファイル名を指定して実行]**コマンドウィンドウが開きます。
2. **[ファイル名を指定して実行]**コマンドウィンドウで、**%appdata%\%trusteer%\rapport\%user%\logs**と入力します。
3. **[OK]**をクリックします。フォルダーが開き、Trusteer Rapportに関連するログファイルのリストが表示されます。
4. **[編集]**メニューで、**[すべて選択]**を選択します。フォルダー内のすべてのファイルが選択されます。
5. マウスを右クリックし、右クリックメニューから**[コピー]**を選択します。
6. ログファイル用のフォルダーを作成します。たとえば、以下のような手順を実行します。

- a. デスクトップでマウスを右クリックして[新規作成]をクリックし、
[フォルダ]を選択します。
- b. フォルダーにLogsという名前を付けます。
7. ログファイル用として作成したフォルダーを開きます。フォルダーアイコンをダブルクリックすれば開きます。
8. 開いたログファイル用のフォルダー内でマウスを右クリックし、右クリックメニューから[貼り付け]を選択します。コピーしたすべてのファイルが、フォルダーに貼り付けられます。
9. Windowsの[スタート]メニューから、再度[ファイル名を指定して実行]をクリックします。再度[ファイル名を指定して実行]コマンドウィンドウが開きます。
- 10.[ファイル名を指定して実行]コマンドウィンドウで、
`%allusersprofile%\application data\trusteer\rapport\logs`と入力します。
- 11.[OK]をクリックします。フォルダーが開き、Trusteer Rapportに関連する別のログファイルのリストが表示されます。
- 12.[編集]メニューで、[すべて選択]を選択します。フォルダー内のすべてのファイルが選択されます。
- 13.マウスを右クリックし、右クリックメニューから[コピー]を選択します。
- 14.作成したログファイル用のフォルダーに戻ります。
- 15.ログファイル用のフォルダー内でマウスをクリックして、先程貼り付けたすべてのファイルが選択されていないことを確認します。
- 16.開いたログファイル用のフォルダー内でマウスを右クリックし、右クリックメニューから[貼り付け]を選択します。2番目にコピーしたログファイルのセットが、フォルダーに貼り付けられます。
- 17.ログファイル用のフォルダーを閉じます。

18. ログファイル用のフォルダー(デスクトップ上または内部にこのフォルダーを作成したフォルダー内)を右クリックして[送る]をクリックし、[圧縮(zip形式)フォルダ]を選択します。zip形式に圧縮されたログファイル用のフォルダーが作成されます。
19. 圧縮されたフォルダーを、電子メールでsupport@trusteer.comに送信します。

18.Trusteer Rapport の最新状態の維持

Trusteer Rapportの有効性を発揮するためには、定期的な更新が必要不可欠です。このため、Trusteer Rapportは自動的に更新を実行します。更新は、ユーザーが認識しないうちに独立して実行されます。さらに、必要なときに随時手動でTrusteer Rapportを更新したり、希望する場合は自動更新を無効にしたりすることもできます。

Trusteer Rapportの更新ステータスのチェック

Trusteer Rapportの更新ステータスに関連する情報は、Rapportコンソール□の[設定]領域に表示されます。

➔ Trusteer Rapportの更新ステータスのチェック方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。[設定]領域は、ダッシュボードの左上に表示されます。

バージョンおよび更新情報

Trusteer Rapport

ダッシュボード

設定

- Rapportは 実行中 (停止)
- アドレスバーアイコン: 表示 (非表示)
- トレイアイコン: 表示 (非表示)
- バージョン: Emerald Build 1302.31
- 保留中の更新: なし(最新の状態)

追加設定

週次アクティビティレポート

ブロックされたスクリーンキャプチャー: 0

証明書の不一致: 0

ブロックされたIPアドレス: 0

フルレポート

信頼されたサイト

信頼されたパートナーのウェブサイト: 299

要注意ウェブサイト: 0

信頼されたウェブサイトの閲覧

ヘルプとサポート

問題の報告

よく寄せられる質問

ユーザーガイド

フィードバックを返す

1/3ページ

[保留中の更新]表示フィールドには、保留中の更新がすべて表示されません。これにより、Trusteer Rapportが最新の状態であるかどうか分かります。ダウンロードされた最終更新が、システムを再起動しないと適用されない場合は、このフィールドに[/はい]と表示されます。

- 任意で、[追加設定]をクリックします。[設定]タブが表示され、詳細情報が表示されます。



更新に関連する表示フィールドは、以下のとおりです。

- **[最終更新クエリー]**: 最後にRapportから新しい更新の有無を問い合わせるクエリーが、最後に送信された日時。
- **[ソフトウェア自動更新]**: 自動更新が有効か無効かを示します。デフォルトは有効です。Trusteerは、すべての更新を確実に受信できるように、デフォルト設定の有効のままにしておくことをお勧めします。

Rapportの手動更新

デフォルトでは、Trusteer Rapportは自動的に更新されます。Trusteer Rapportを手動で更新することもできます。

➔ Trusteer Rapportの手動更新方法

1. [「Rapportコンソールのオープン」](#) (72ページ)を参照して、Rapportコンソールを開きます。[設定]領域は、ダッシュボードの左上に表示されます。

バージョンおよび更新情報

Trusteer Rapport

ダッシュボード

設定

- Rapportは 実行中 (停止)
- アドレスバーアイコン: 表示 (非表示)
- トレイアイコン: 表示 (非表示)
- バージョン: Emerald Build 1302.31
- 保留中の更新: なし(最新の状態)

追加設定

週次アクティビティレポート

ブロックされたスクリーンキャプチャー: 0

証明書の不一致: 0

ブロックされたIPアドレス: 0

フルレポート

信頼されたサイト

信頼されたパートナーのウェブサイト: 299

要注意ウェブサイト: 0

信頼されたウェブサイトの閲覧

ヘルプとサポート

問題の報告

よく寄せられる質問

ユーザーガイド

フィードバックを返す

1 / 3 ページ

2. [追加設定]をクリックします。[設定]タブが表示されます。



3. [今すぐ更新をチェックする]をクリックします。Trusteer Rapportが、更新の有無を確認します。更新の有無の確認中、進行状況が表示フィールドの下に表示されるテキストによって示されます。以下のいずれかが発生します。

- Trusteer Rapportは、保留中の更新を検知しませんでした。この場合、[最新の設定情報で動作しています]というメッセージが表示されます。
- Trusteer Rapportは、更新を検知し、ダウンロードして適用しました。この場合、[設定情報が更新されました。最新の設定情報で動作しています]というメッセージが表示されます。[設定ファイル]表示フィールドの番号は、1つずつ大きくなります。

- Trusteer Rapportは、更新を検知し、ダウンロードしました。更新は再起動後に適用されます。この場合、[ソフトウェア更新の準備中 設定情報は最新です]というメッセージが表示されます。**[保留中の更新]**表示フィールドが[はい、PCを再起動します]に変わります。
- Trusteer Rapportは、複数の更新を検知し、ダウンロードしました。一部の更新はただちに適用され、残りはコンピューターの再起動後に適用されます。この場合、[ソフトウェア更新の準備中 設定情報は更新されました]というメッセージが表示されます。**[設定ファイル]**表示フィールドの番号は、1つずつ大きくなります。**[保留中の更新]**表示フィールドが[はい、PCを再起動します]に変わります。

自動更新の無効化

デフォルトでは、Trusteer Rapportは自動的に更新を実行します。更新は、ユーザーが認識しないうちに独立して実行されます。Trusteer Rapportの有効性を発揮するためには、定期的な更新が必要不可欠です。Trusteerでは、自動更新の無効化は推奨しません。

➔ 自動更新の無効化方法

1. 「[Rapportコンソールのオープン](#)」(72ページ)を参照して、Rapportコンソールを開きます。[設定]領域は、ダッシュボードの左上に表示されません。

バージョンおよび更新情報

Trusteer Rapport

ダッシュボード

設定

- Rapportは 実行中 (停止)
- アドレスバーアイコン: 表示 (非表示)
- トレイアイコン: 表示 (非表示)

バージョン: Emerald Build 1302.31
保留中の更新: なし(最新の状態)

追加設定

週次アクティビティレポート

ブロックされたスクリーンキャプチャー: 0

証明書の不一致: 0

ブロックされたIPアドレス: 0

フルレポート

信頼されたサイト

信頼されたパートナーのウェブサイト: 299

要注意ウェブサイト: 0

信頼されたウェブサイトの閲覧

ヘルプとサポート

問題の報告

よく寄せられる質問

ユーザーガイド

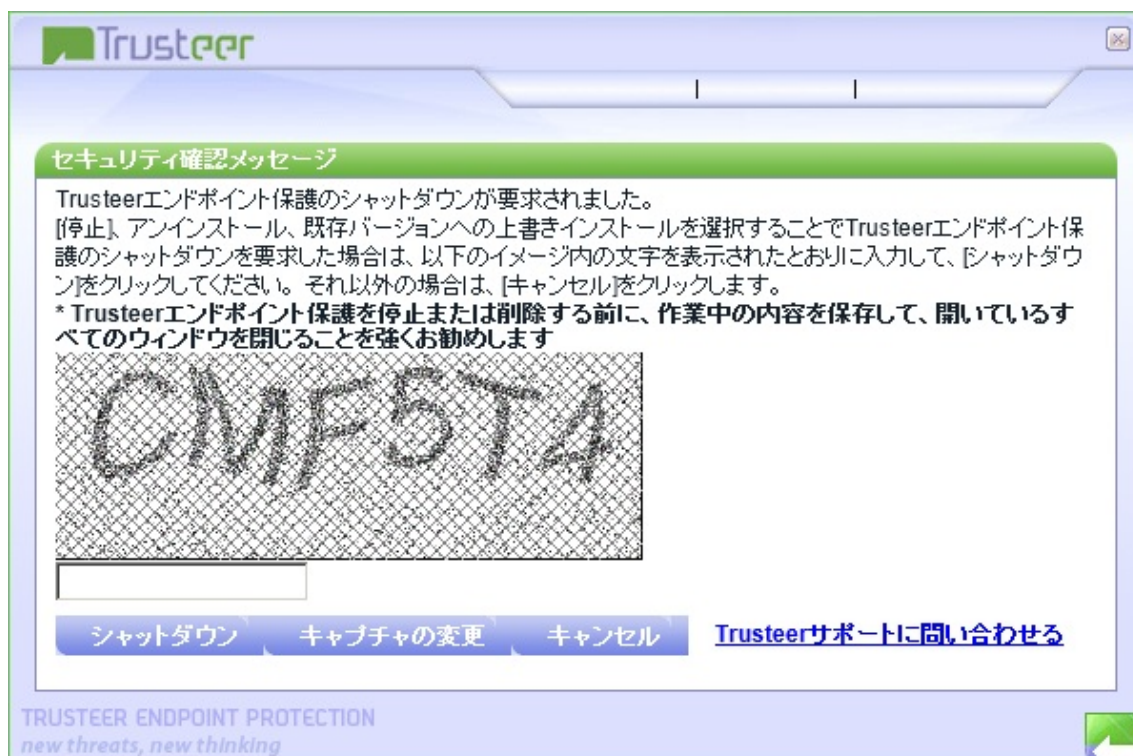
フィードバックを返す

1 / 3 ページ

2. [追加設定]をクリックします。[設定]タブが表示されます。



3. [ソフトウェア自動更新]チェックボックスをオフにします。[ユーザーによる許可]タブが開きます。この画面には、ユーザーが入力する文字が表示された画像が表示されます。これは、マルウェアがコンソールにアクセスし、効果的にTrusteer Rapportを無効にしてしまうことを防ぐためのものです。



4. 画像に表示された文字を入力します。
5. [OK]をクリックします。自動更新が無効になります。自動更新が無効になっている間は、[「Rapportの手動更新」](#) (243ページ) を実行しない限り、Trusteer Rapportは更新されません。

19.Trusteer Rapport のアンインストール

Trusteer Rapportは、アンインストールしないことを強くお奨めします。Trusteer Rapportで問題が発生している場合は、サポートのリクエストを <http://www.trusteer.com/support/submit-ticket> に送信していただくことをお奨めします。問題を解決する間は、アンインストールするのではなく、[「Trusteer Rapportの停止」](#) (207ページ)を実施します。

Trusteer Rapportでは、1種類のアンインストール方法のみをサポートとしています。これは、不正なアンインストールからTrusteer Rapportを保護するためです。

注: Trusteer RapportをWindowsの管理者アカウントからインストールした場合、管理者アカウントにログインしている場合のみ、Trusteer Rapportをアンインストールできます。

Trusteer Rapport のアンインストール(Windows 7)

➔ Trusteer Rapportのアンインストール方法

1. コントロールパネルを開きます。
2. **[すべてのプログラム]**の下にある**[プログラムのアンインストール]**をクリックします。
3. プログラムの一覧の中からTrusteer Rapportを見つけ、**[Rapport]**をダブルクリックします。確認メッセージが表示されます。
4. **[はい]**をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。
5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。

6. **[いいえ、今すぐアンインストールする]**をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

Trusteer Rapport のアンインストール(Windows XP)

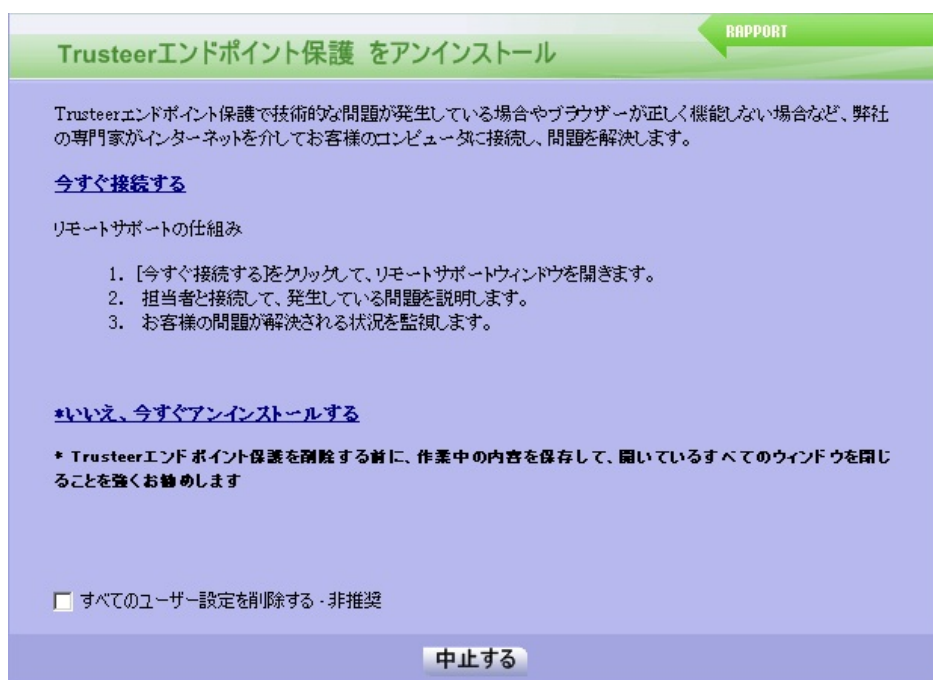
➔ Trusteer Rapportのアンインストール方法

1. コントロールパネルを開きます。
2. **[アプリケーションの追加と削除]**をクリックします。
3. プログラムの一覧の中からTrusteer Rapportを見つけ、Trusteer Rapportに対する**[変更と削除]**ボタンをクリックします。確認メッセージが表示されます。
4. **[はい]**をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。
5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。
6. **[いいえ、今すぐアンインストールする]**をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

注: Trusteer Rapportのアンインストールで問題が発生した場合は、<http://www.trusteer.com/book/uninstalling-rapport-using-safeuninstall-utility>にアクセスし、安全なアンインストールユーティリティを使用してTrusteer Rapportをアンインストールする情報について確認してください。

アンインストール画面の[すべてのユーザー設定を削除する]チェックボックスについて

以下の画面に表示される[すべてのユーザー設定を削除する]チェックボックスは、Trusteer Rapportに加えたすべての変更を削除するものです。これには、追加したサイトや、保護することを選択したパスワードが含まれます。このチェックボックスをオンにしてからTrusteer Rapportを再インストールした場合、Trusteer Rapportにユーザーが加えた変更は破棄されます。



Trusteer Rapport のアンインストール(Windows 7)

➔ Trusteer Rapportのアンインストール方法

1. コントロールパネルを開きます。
2. [すべてのプログラム]の下にある[プログラムのアンインストール]をクリックします。

3. プログラムの一覧の中からTrusteer Rapportを見つけ、**[Rapport]**をダブルクリックします。確認メッセージが表示されます。
4. **[はい]**をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。
5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。
6. **[いいえ、今すぐアンインストールする]**をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

Trusteer Rapport のアンインストール(Windows XP)

➔ Trusteer Rapportのアンインストール方法

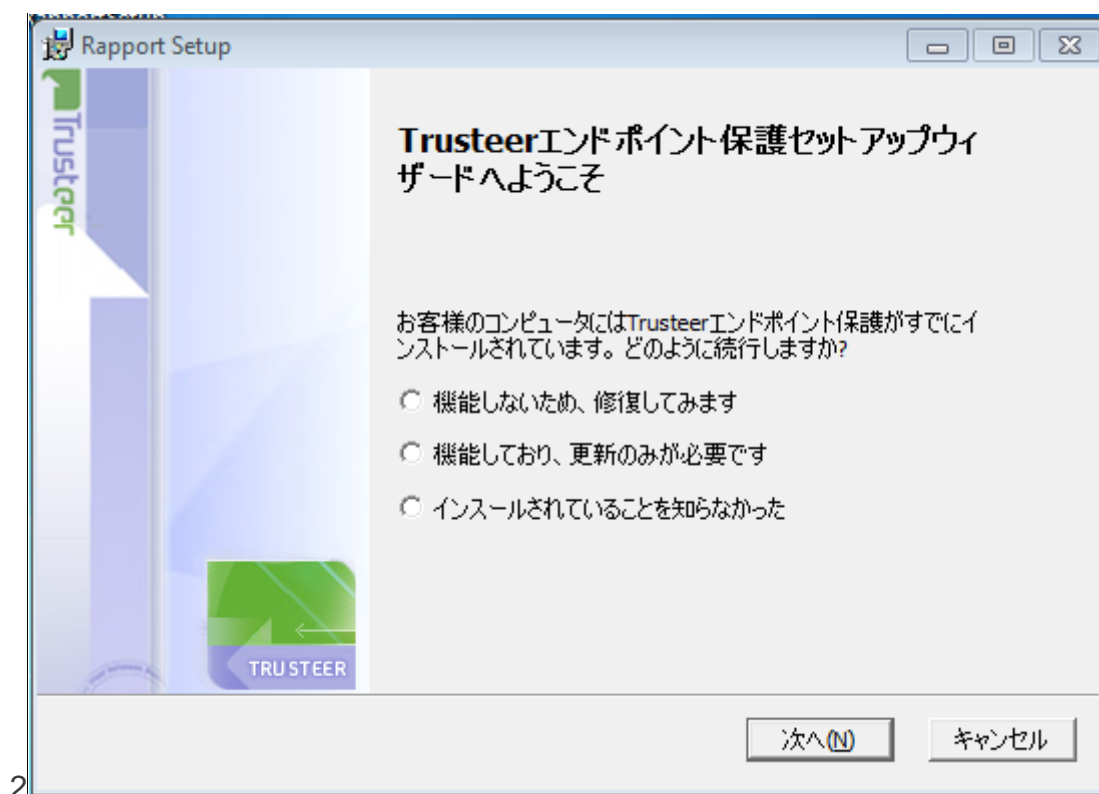
1. コントロールパネルを開きます。
2. **[アプリケーションの追加と削除]**をクリックします。
3. プログラムの一覧の中からTrusteer Rapportを見つけ、Trusteer Rapportに対する**[変更と削除]**ボタンをクリックします。確認メッセージが表示されます。
4. **[はい]**をクリックします。Trusteer Rapportが正常に防止した最近のイベントを示したTrusteer Rapportのダイアログボックスが表示されます。

5. **[続行する]**をクリックします。別のTrusteer Rapportのダイアログボックスが表示され、Trusteer Rapportで発生した可能性のある技術的な問題についてのサポートが提案されます。アンインストールの操作を続行する前に、開いているすべてのファイルおよびアプリケーションを閉じてください。
6. **[いいえ、今すぐアンインストールする]**をクリックします。要求に応じて、Trusteer Rapportのアンインストールが完了します。アンインストールが完了すると、新しいブラウザーウィンドウが開き、Trusteer Rapportについてのフィードバックと、いくつかの基本的な質問に回答するように求められます。

20. Trusteer Rapport のアップグレード

新しいバージョンのTrusteer Rapportにアップグレードするには、古いバージョンを削除せず、新しいバージョンをインストールするだけで済みます。インストールのプロセスは、通常のインストールプロセスに、いくつかの追加ステップが入ります。

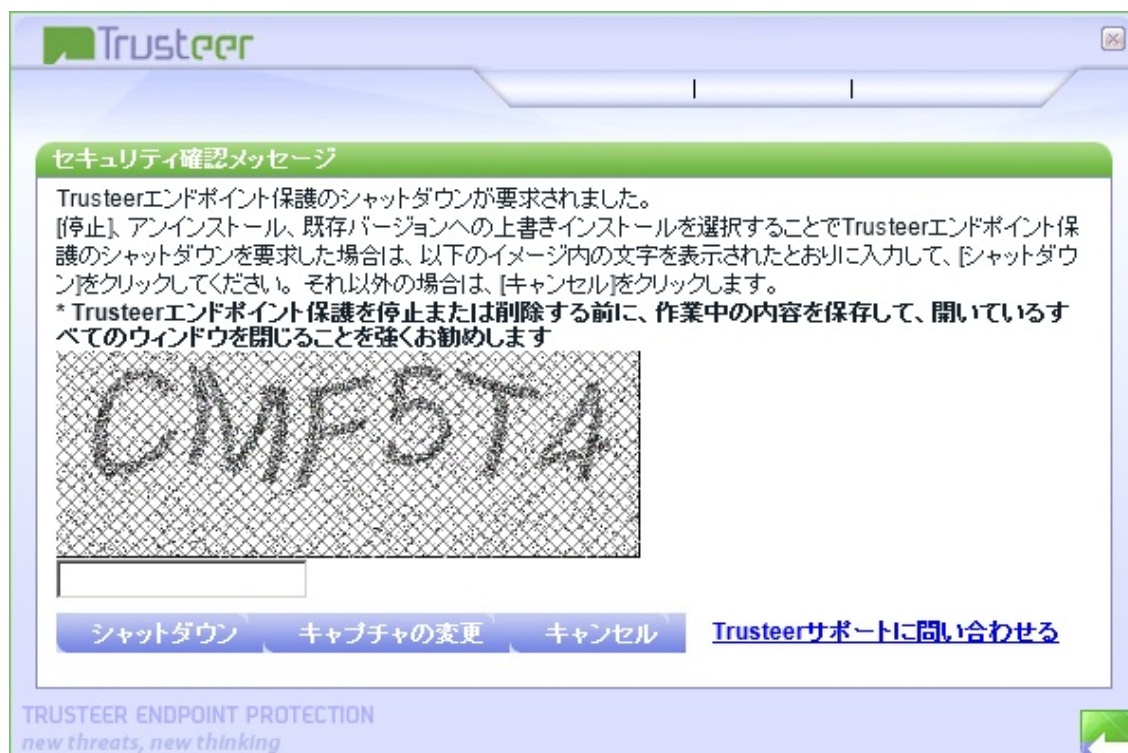
新しいバージョンのRapportにアップグレードするには、通常と全く同じ方法でインストールします。インストール手順の詳細については、「[Trusteer Rapportのインストール](#)」(27ページ)を参照してください。インストール中は、以下の画面が表示されます。



この画面は、既存のバージョンの上に新しいバージョンをインストールしているために表示されます。この画面が表示されたら、**[機能しており、更新のみが必要です]**を選択します。その後、**[次へ]**をクリックして通常のインストールを続行します。

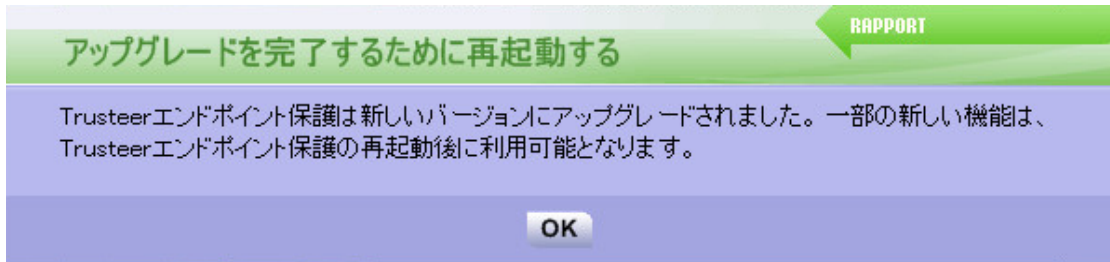
注: Trusteer Rapportを管理者レベルのWindowsアカウントからインストールした場合、管理者アカウントにログインしている場合のみ、既存のバージョンの上にTrusteer Rapportをインストールできます。

インストールプロセス中に、以下の画面も表示されます。



この画面は、設定ウィザードでは、新しいバージョンをインストールするために、既存のバージョンのTrusteer Rapportをシャットダウンする必要があるため表示されています。シャットダウンには、ユーザーの確認が必要です。これは、マルウェアによりTrusteer Rapportが無効化されることを防ぐためのものです。この画面が表示されたら、画像に表示されている文字を入力して、[シャットダウン]をクリックします。インストールが通常どおりに続行されます。

インストール後、以下の画面が表示される場合があります。



このメッセージが表示された後も、ご使用のコンピューターは安全です。ただし、できるだけ早くコンピューターを再起動することをお奨めします。