










MRB-Cloud 設定マニュアル

・全体目次




基本設定 P. 3

-  1 ログイン
-  2 ログインパスワードの変更
-  3 セキュリティ設定
-  4 ホワイトリスト申請/処理
-  5 管理者登録



HTTPSフィルタリング P. 33

-  1 HTTPSフィルタリング設定
-  2 証明書のダウンロード
-  3 証明書のインポート
-  4 クライアント証明書を利用する場合

メールフィルタリング P. 54

-  1 Outlookの設定確認
-  2 MRBの設定
-  3 SSLでメールを受信している場合

その他の項目 P. 78

-  1 グループ設定
-  2 ログ閲覧

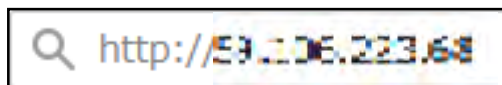
基本設定

・基本設定 目次

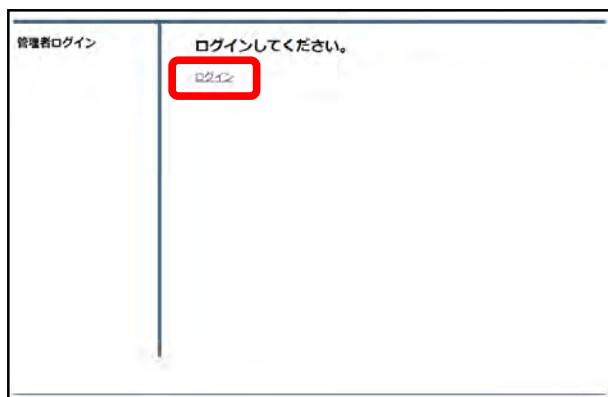
1	ログイン	P. 5
2	ログインパスワードの変更	P. 8
3	セキュリティ設定	P. 11
3-1	URLフィルタリング	
3-2	URLフィルタリング(カスタムカテゴリ)	
3-3	個別URLフィルタリング	
3-4	IPフィルタリング	
3-5	個別IPフィルタリング	
4	ホワイトリスト申請/処理	P. 26
4-1	ホワイトリスト申請	
4-2	ホワイトリスト申請処理	
5	管理者登録	P. 31

1, ログイン

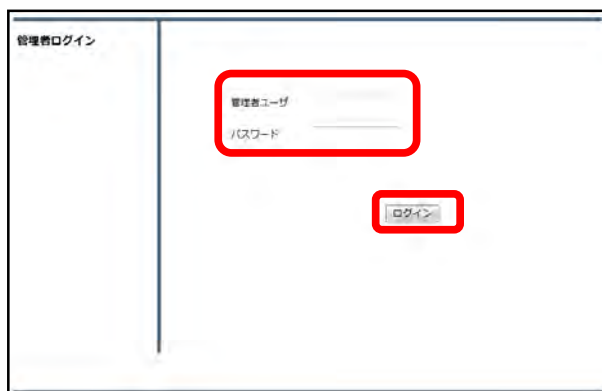
MRBの操作を行うために管理コンソールにログインします。



①管理コンソールにログインするため、ブラウザのURL入力部分にMRB-CloudのIPアドレスを入力し、確定(Enter)してください。



②左のような画面が表示されましたら『ログイン』をクリックしてください。



③管理者ユーザ欄に『root』、パスワード欄に『mr-5』と入力し、『ログイン』をクリックしてください。

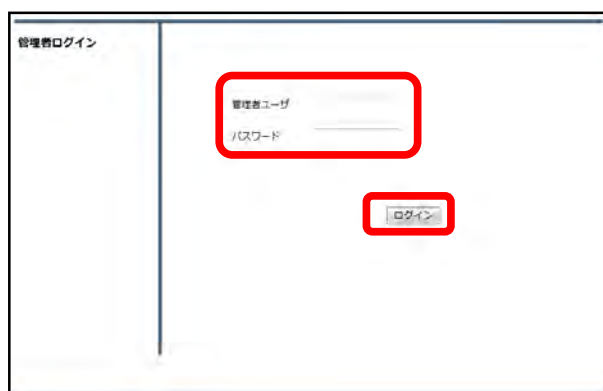


④左のような画面が表示されましたら、ログイン作業は完了です。

※管理者ユーザ/パスワードを正しく入れてもログイン出来ない場合。



⑤ブラウザのURL入力欄に『http://“MRB-CloudのIPアドレス”/show_login2.cgi』と入力し、確定(Enter)してください。



⑥左のようにログイン画面が表示されましたら、通常と同様に管理ユーザに『root』、パスワードに『mr-5』と入力してください。

2, ログインパスワード の変更

セキュリティ向上の為、 管理コンソールへのログインパスワードを変更します。



①管理画面にログインをし、右上の『設定』をクリックします。



②左下の『パスワード変更』をクリックします。



③入力欄に新しいパスワードを入力し、
『変更』をクリックします。
(パスワードは8～16文字で設定してください)

管理者ログイン

管理者ユーザ

パスワード

ログイン

④設定後、ログイン画面が出てきますので、新しいパスワードを入力し、『ログイン』をクリックしてください。

890003 クラウドテスト-890003

表示/確認 設定 ログアウト

表示/確認

バージョン

セキュリティ設定

URLフィルタリング

IPフィルタリング

振る舞い検知

HTTPS通信

メール設定

ホワイトリスト検知

情報

ログ

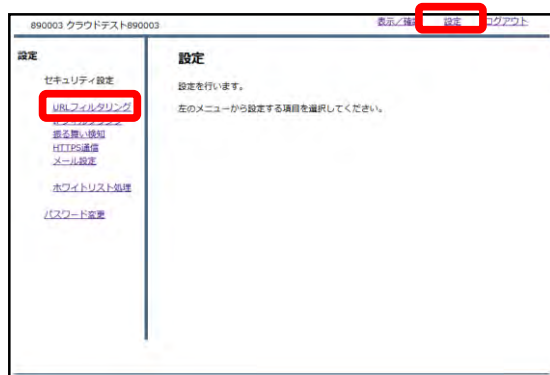
バージョン	
ソフトウェア	1.0.1
URLフィルタリング	1.0.1
IPフィルタリング	1.0.1
振る舞い検知	1.0.1

⑤ログインに成功すれば、パスワード変更作業は完了です。

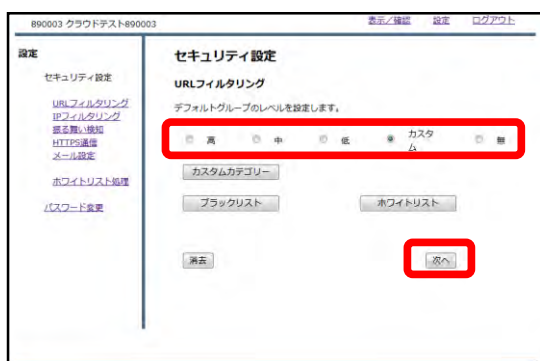
3, セキュリティ設定

URLフィルタリング

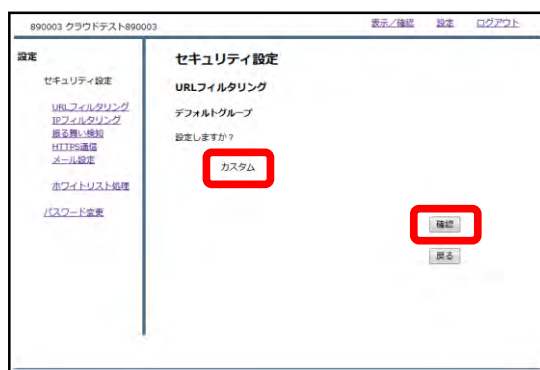
URLフィルタの強度設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『URLフィルタリング』をクリックします。



②ラジオボタンよりフィルタリングのレベルを選択し、『次へ』をクリックします。



③設定を確認し、正しければ『確認』をクリックして設定は完了です。

URLフィルタリング (カスタムカテゴリ)

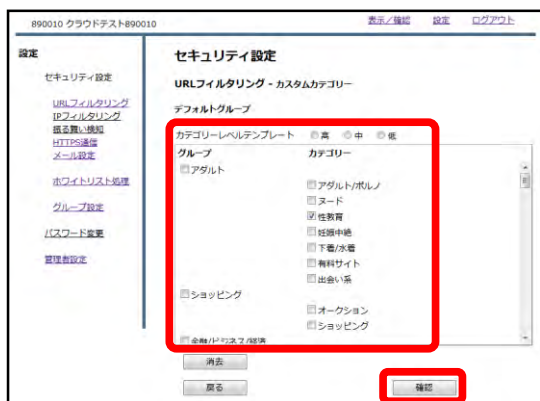
URLフィルタのカスタム設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『URLフィルタリング』をクリックします。



②『カスタムカテゴリ』をクリックします。



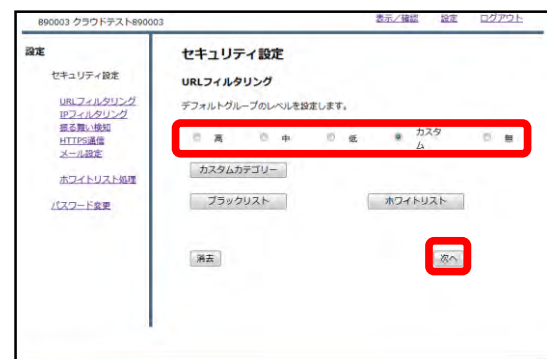
③チェックボックスでブロックしたいカテゴリを選択し、『確認』をクリックします。



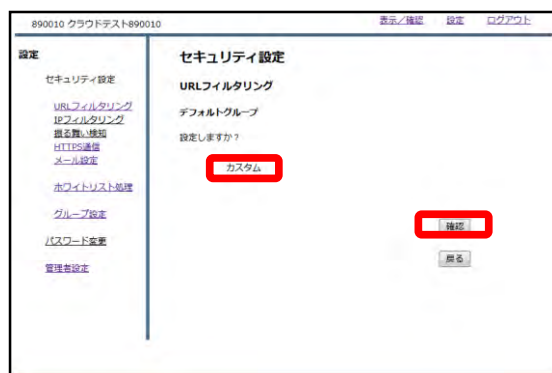
④選択項目を確認し、よければ『設定』をクリックします。



⑤『戻る』をクリックします。



⑥ラジオボタンより“カスタム”を選択し、『次へ』をクリックします。



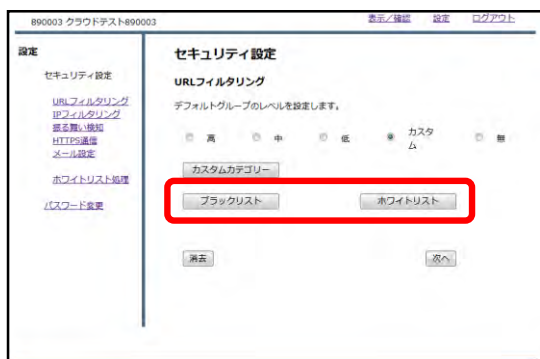
⑦設定を確認し、正しければ『確認』をクリックして設定は完了です。

個別URLフィルタリング 登録

特定のURLに対してのブロック/スルーの設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『URLフィルタリング』をクリックします。



②指定するURLをブロックする場合は『ブラックリスト』、ブロックを解除する場合は『ホワイトリスト』をクリックします。



③『追加』をクリックします。



④記入欄にブロック/スルーしたいURLを入力し、『追加』をクリックします。

※http://は入力しないでください。



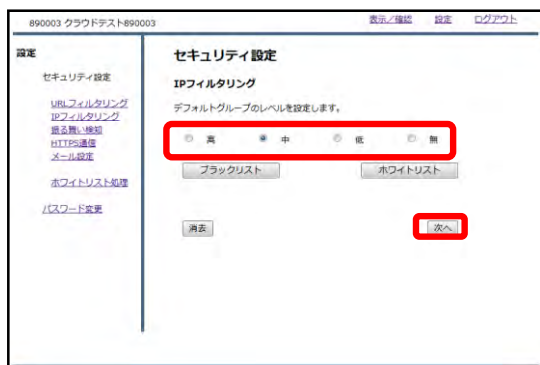
⑤URLを確認し、正しければ『追加』をクリックして設定は完了です。

IPフ ィルタ リ ング

IPフィルタの強度設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『IPフィルタリング』をクリックします。



②ラジオボタンよりフィルタリングのレベルを選択し、『次へ』をクリックします。



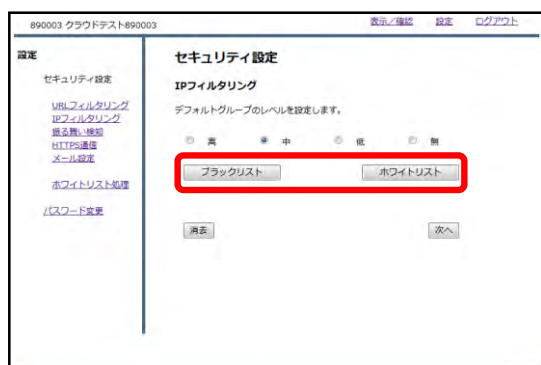
③設定を確認し、正しければ『確認』をクリックして設定は完了です。

個別IPフィルタリング 登録

特定のIPに対してのブロック/スルーの設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『IPフィルタリング』をクリックします。



②指定するIPをブロックする場合は『ブラックリスト』、ブロックを解除する場合は『ホワイトリスト』をクリックします。



③『追加』をクリックします。



④記入欄にブロック/スルーしたいIPを入力し、『追加』をクリックします。

※ネットワーク単位で指定する場合は、IPの後ろに"/24"などのマスクを追加してください。



⑤IPを確認し、正しければ『追加』をクリックして設定は完了です。

4, ホワイトリスト 申請/処理

ホワイトリスト申請

閲覧しようとしたWebサイトがブロックされている場合、管理者の方へブロック解除の申請を行うことができます。

URLフィルターによりブロックされました。

サイト	http://www.sourdeneta.com
フィルター	持ちノリ
IPアドレス	192.168.150.10

サイトの再評価を申請

今回のみ接続を許可

ホワイトリストに登録を申請

サイトの再評価をします。
解放されるまでに、数日費します。
(全てのMRB-CLOUDに反映されます。)

ご注意ください。
10分間アクセス可能になります。
また同じカテゴリーのページも閲覧可能になり、ログが残ります。

管理者としての設定が必要です。
管理者の方に伝えてください。
(このMRB-CLOUDのみ反映されます。)

①Webサイトがブロックされた場合、左のような画面が表示されます。右下『ホワイトリストに登録を申請』をクリックしてください。

ホワイトリストに登録を申請しました。管理者の方に連絡してください。

対象URL	http://www.sourdeneta.com
-------	---

②左のような画面が表示されましたら、申請は完了です。管理者の方に連絡してください。

ホワイトリスト 申請処理

管理者の方は利用者からのWebサイトアクセス許可の申請に対して処理を行うことができます。



①管理画面にログイン後、右上の『設定』をクリックし、左の『ホワイトリスト処理』をクリックします。



②申請があったWebサイトに対して、ラジオボタンにより”許可”、”拒否”を選択し、『設定』をクリックします。



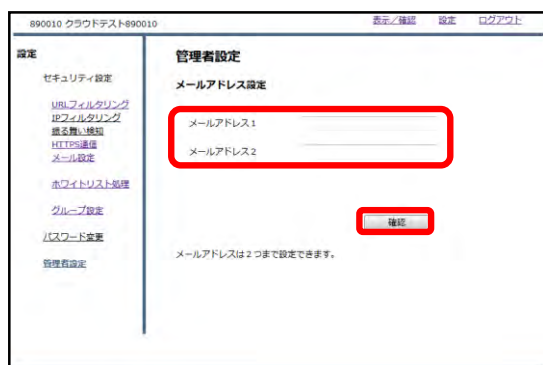
③内容を確認し、正しければ『設定』をクリックして処理は完了です。

5, 管理者登録

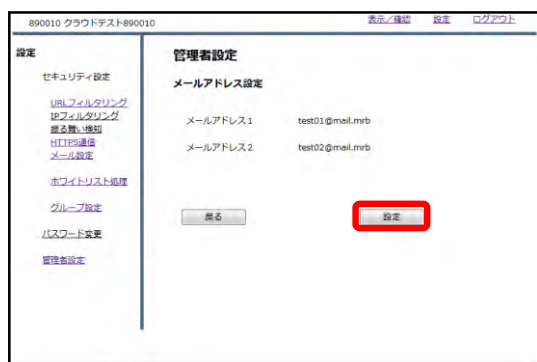
レポートメールを受信するメールアドレスを設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左の『管理者設定』をクリックします。



②メールアドレスを記入し、『確認』をクリックします。



③内容を確認し、正しければ『設定』をクリックして処理は完了です。

HTTPS フィルタリング

・HTTPSフィルタリング設定 目次

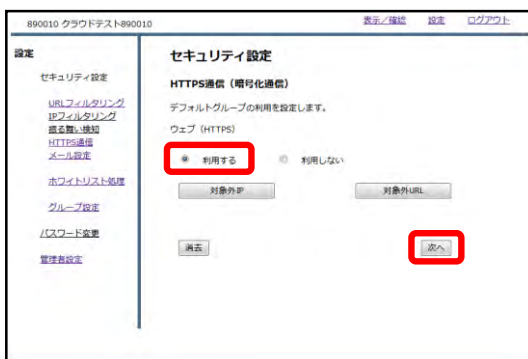
1	<u>MRBの設定</u>	P. 35
2	<u>証明書のダウンロード</u>	P. 37
3	<u>PCの設定</u>	P. 39
3-1	IE/Chromeの場合	
3-2	FireFoxの場合	
4	<u>クライアント証明書を利用する場合</u>	P. 47
4-1	対象外URL設定	
4-2	対象外IP設定	

1, MRBの設定

HTTPSフィルタリング機能により、暗号化されたWebサイトもフィルタリングが可能になります。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『利用する』を選択し、『次へ』をクリックします。



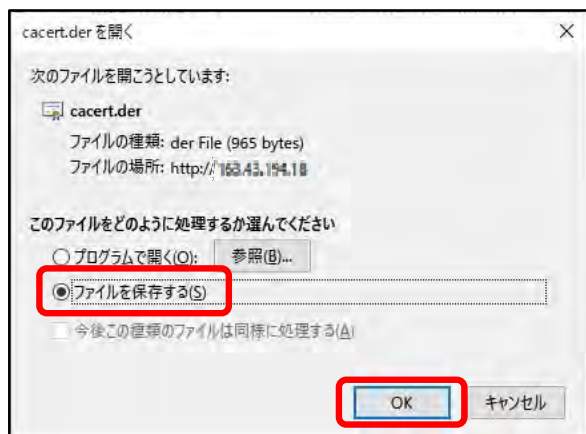
③『確認』をクリックして設定は完了です。

2, 証明書の ダウンロード

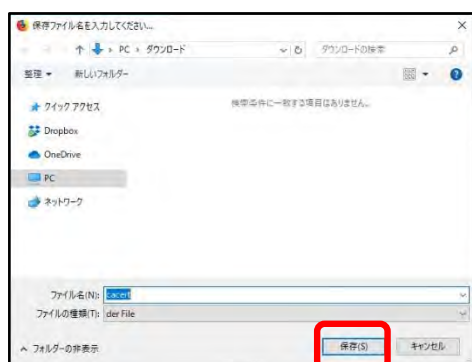
HTTPSフィルタリング機能で使用する証明書をダウンロードします。



①管理画面にログイン後、左側『情報』をクリックし、『証明書ダウンロード』をクリックします。



②左のようなダイアログが表示されたら、ラジオボタンより『ファイルを保存する』を選択し、『OK』をクリックします。



③分かりやすいフォルダ(デスクトップ等)に移動し、『保存』をクリックしましたら、証明書のダウンロードは完了です。

3, PCの設定

IE/Chrome利用の場合

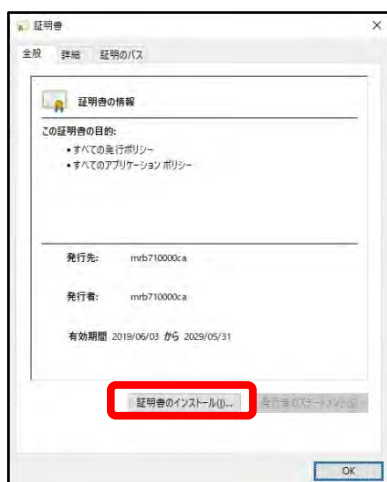
IEまたはChromeをご利用の場合、ダウンロードしたMRBの証明書をインポートする手順です。



①ダウンロードした証明書をダブルクリックします。



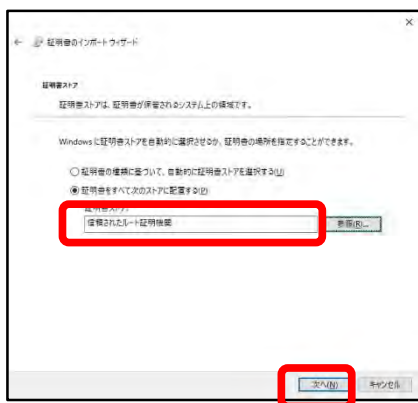
②左のようなダイアログが表示されますので、『開く』をクリックします。



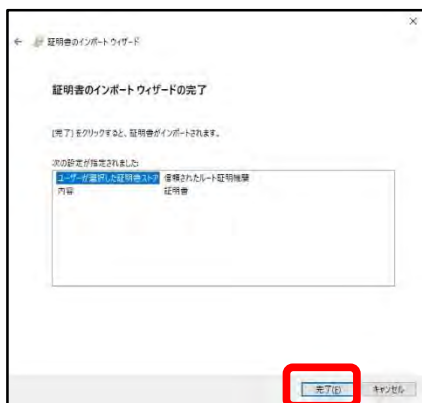
③『証明書のインストール』をクリックします。



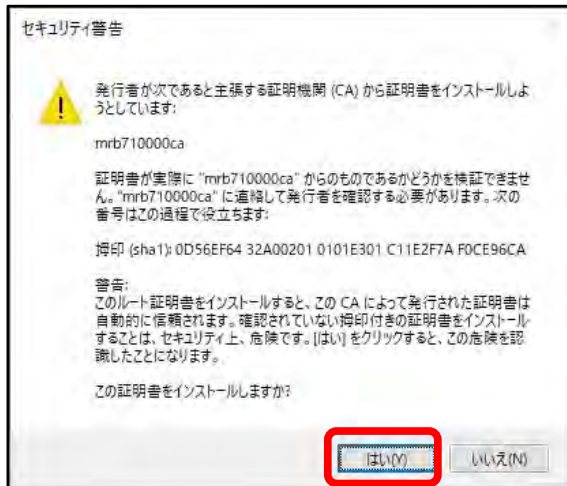
④左のようなポップアップが表示されますので、『次へ』をクリックします。



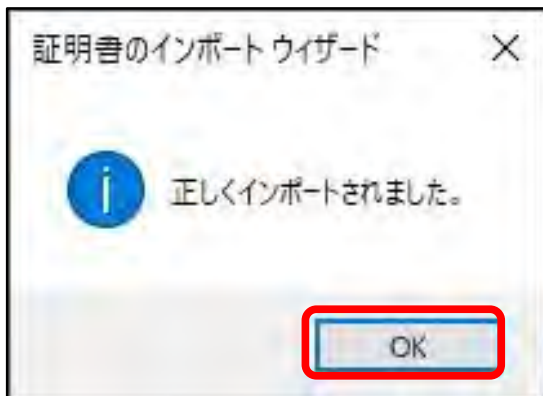
⑤ラジオボタンより『証明書をすべて次のストアに配置する』を選択し、『参照』より“信頼されたルート証明機関”を選択して『次へ』をクリックします。



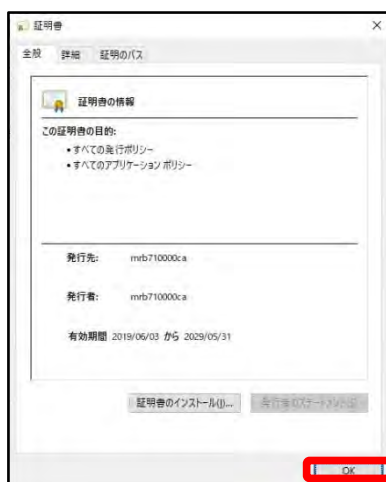
⑥内容を確認し、正しければ『完了』をクリックします。



④左のような警告が表示されますが、『はい』をクリックします。



⑦左のようなポップアップが表示されましたら『OK』をクリックします。



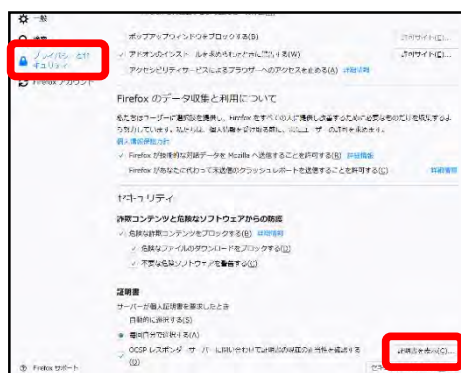
⑧『OK』をクリックして証明書のインポート作業は完了です。

FireFox利用の場合

Firefoxをご利用の場合、ダウンロードしたMRBの証明書をインポートする際の手順です。



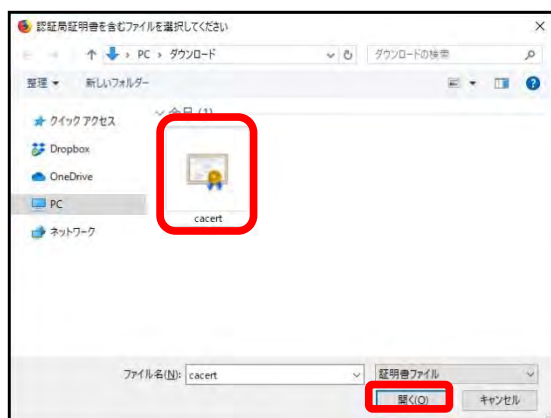
①Firefoxのブラウザを開き、右上の『メニュー』より『オプション』を選択します。



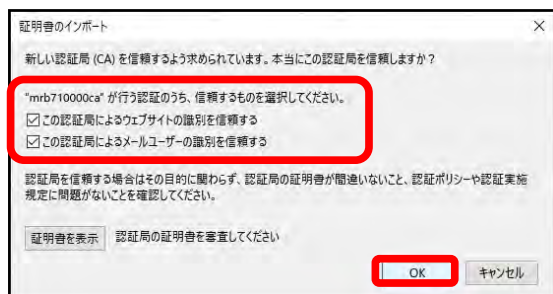
②左側『プライバシーとセキュリティ』をクリックし、『証明書を表示』をクリックします。



③ポップアップが表示されましたら、『認証局証明書』タブより『インポート』をクリックします。



④ダイアログが表示されますので、ダウンロードした証明書を選択し、『開く』をクリックします。



⑤表示される2つのチェックボックスの全てにチェックを入れて『OK』をクリックします。



⑥証明書一覧に発行者名"Technol"の『mrb...』という証明書があることを確認したら、証明書のインポートは完了です。

4, クライアント証明書 を利用する場合

対象外URL設定

HTTPSフィルタリングを活用している際にネットバンキング等でクライアント証明書を使用する場合に行う設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『対象外URL』をクリックします。



③『追加』をクリックします。

890010 クラウドテスト-890010

表示/確認 設定 ログアウト

設定

セキュリティ設定

URLフィルタリング
IPフィルタリング
アクセス制御
HTTPプロキシ
メール設定
ホストリスト処理
グループ設定
パスワード管理
管理者設定

セキュリティ設定

HTTPS 対象外URL

デフォルトグループ

正規表現を利用する事ができます。

URL test.mrb

追加

戻る

④URL記入欄にクライアント証明書を使用するサイトのURLを入力し、『追加』をクリックします。

※http://の入力は不要です。

890010 クラウドテスト-890010

表示/確認 設定 ログアウト

設定

セキュリティ設定

URLフィルタリング
IPフィルタリング
アクセス制御
HTTPプロキシ
メール設定
ホストリスト処理
グループ設定
パスワード管理
管理者設定

セキュリティ設定

HTTPS 対象外URL

デフォルトグループ

設定しますか？

URL	test.mrb
-----	----------

追加

戻る

⑤入力したURLを確認し、正しければ『追加』をクリックして設定は完了です。

対象外IP設定

HTTPSフィルタリングを活用している際にネットバンキング等でクライアント証明書を使用する場合に行う設定です。



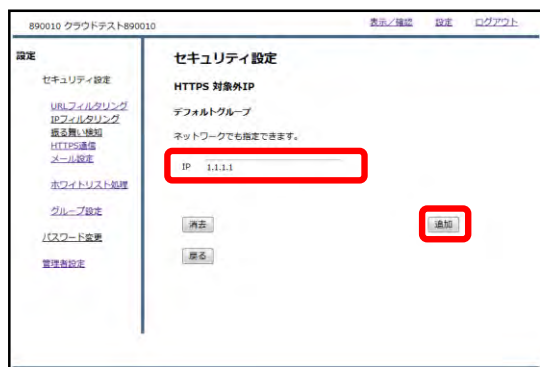
①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『対象外IP』をクリックします。



③『追加』をクリックします。



④IP記入欄にクライアント証明書を使用するサイトのIPアドレスとサブネットマスク長を入力し、『追加』をクリックします。

※サブネットマスク長は入力を省略した場合、32に設定されます。



⑤入力したIPアドレスを確認し、正しければ『追加』をクリックして設定は完了です。

メールフィルタリング

・メールフィルタリング設定 目次

※現在動作を保証しているのはOutlookのみです。

1 Outlookの設定確認 P. 56

1-1 メールアカウント設定の確認

2 MRBの設定 P. 61

2-1 メール検疫機能の設定

2-2 許可アドレス設定

2-3 検知アドレス設定

3 SSLでメール受信をご利用の場合 P. 71

3-1 証明書のダウンロード

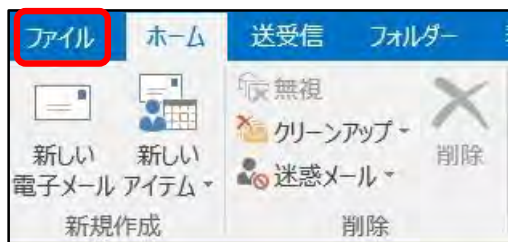
3-2 証明書の導入

1, Outlookの設定確認

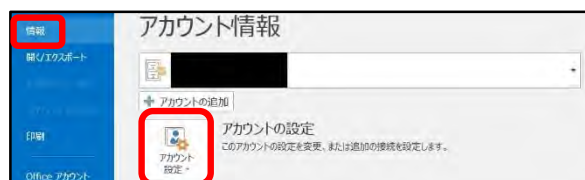
メールアカウント設定 の確認

MRBの設定を行う前にOutlookでのメール設定を確認します。

①Outlookを起動し、左上の『ファイル』をクリックします。



②『情報』タブより『アカウントの設定』をクリックします。



③設定を行うメールアドレスをダブルクリックします。





④ 『詳細設定』 をクリックします。



⑤ 『詳細設定』 タブを開き、“受信サーバー”の“使用する暗号化接続の種類”を確認します。

『SSL/TLS』もしくは『STARTTLS』と指定されていた場合は**“3,SSLでメール受信をご利用の場合”**に従って証明書のインポート作業を行って下さい。
確認後、『OK』をクリックします。



⑥ 『次へ』 をクリックします。



⑦接続確認が行われますので、終了後『閉じる』を押して確認作業は完了です。

2, MRBの設定

メール検疫機能の設定

MRBを経由するメールを検疫するための設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。



②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③スパム検知、ウイルス検知を利用する場合はそれぞれのラジオボタンより『利用する』を選択し、メールの受信をSSLで行っている場合はセキュア通信のラジオボタンより『利用する』を選択して『次へ』をクリックします。

※スパム検知は送信元アドレス、ウイルス検知は添付ファイルをそれぞれチェックします。

890010 クラウドテスト-890010 設定の確認 設定 ログアウト

設定

セキュリティ設定

URLフィルタリング
IPフィルタリング
送信元IP通知
SMTPの通知
メール設定
ホワイトリスト設定
グループ設定
パスワード変更
管理画設定

セキュリティ設定

メール設定

デフォルトグループ

設定しますか？

メール受信 (IMAP, POP3)	利用する
スパム検知機能	利用する
スパム表示件名	-SPAM-
ウイルス検知機能	利用する
ウイルス表示件名	-VIRUS-
セキュア通信	利用しない

確認

戻る

④設定内容を確認し、正しければ『確認』をクリックして設定は完了です。

許可アドレス設定

信頼できる宛先がスパムメールと判定される場合、許可アドレスとして設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。



②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③『許可アドレス』をクリックします。



④『追加』をクリックします。



⑤メールアドレス記入欄にスパム判定から除外するメールアドレスを入力し、『追加』をクリックします。



⑥入力したメールアドレスを確認し、正しければ『追加』をクリックして設定は完了です。

検知アドレス設定

スパムメールとして判定させたいメールアドレスが存在する場合、
検知アドレスとして設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。



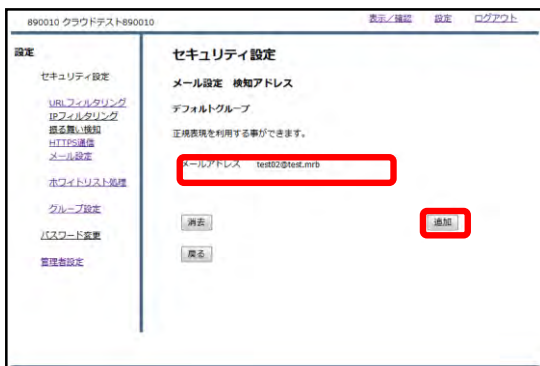
②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③『スパム検知アドレス』をクリックします。



④『追加』をクリックします。



⑤メールアドレス記入欄にスパムとして検知させたいメールアドレスを記入し、『追加』をクリックします。



⑥入力したメールアドレスを確認し、正しければ『追加』をクリックします。

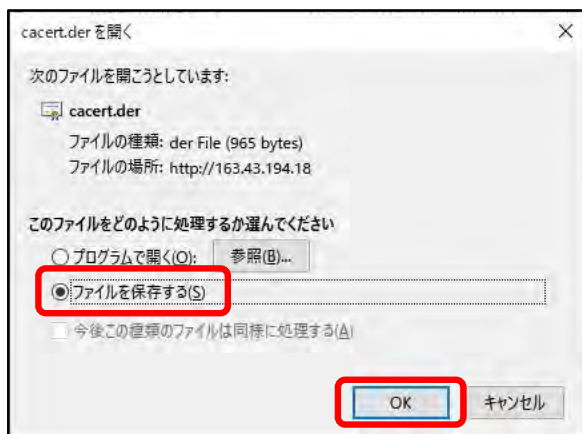
3, SSLでメール受信を ご利用の場合

証明書のダウンロード

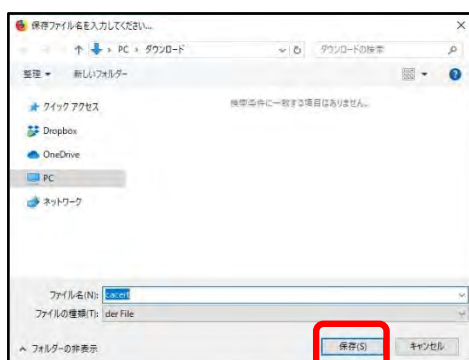
SSLで受信したメールを検疫する際の証明書をダウンロードします。



①管理画面にログイン後、左側『情報』をクリックし、『証明書ダウンロード』をクリックします。



②左のようなダイアログが表示されたら、ラジオボタンより『ファイルを保存する』を選択し、『OK』をクリックします。



③分かりやすいフォルダ(デスクトップ等)に移動し、『保存』をクリックしましたら、証明書のダウンロードは完了です。

証明書のインポート

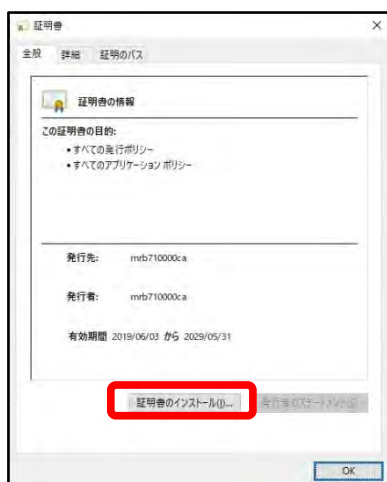
SSLで受信したメールを検疫する際、ダウンロードしたMRBの証明書をインポートする際の手順です。



①ダウンロードした証明書をダブルクリックします。



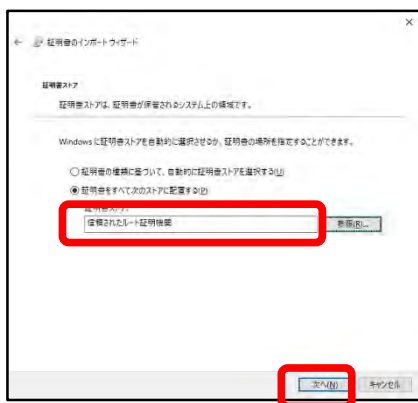
②左のようなダイアログが表示されますので、『開く』をクリックします。



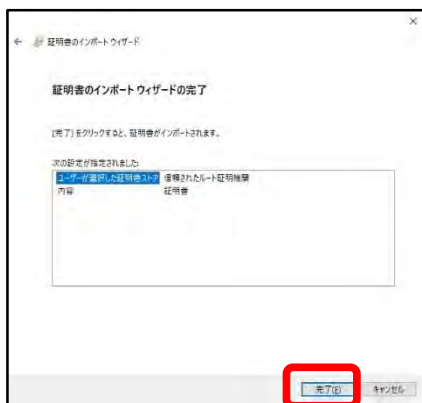
③『証明書のインストール』をクリックします。



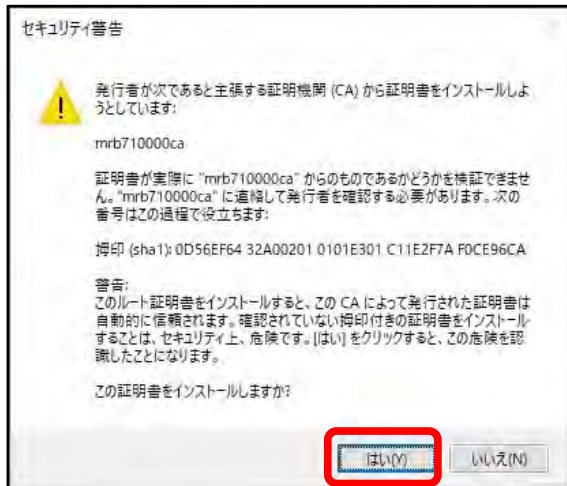
④左のようなポップアップが表示されますので、『次へ』をクリックします。



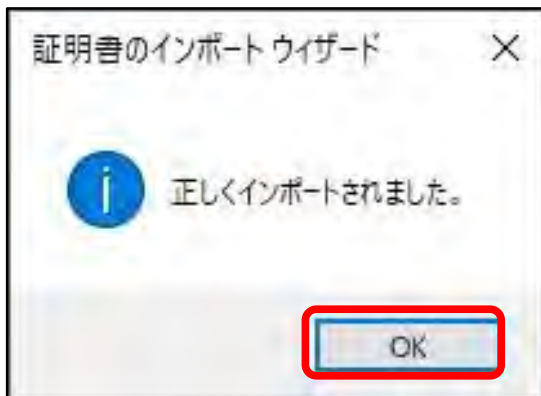
⑤ラジオボタンより『証明書をすべて次のストアに配置する』を選択し、『参照』より“信頼されたルート証明機関”を選択して『次へ』をクリックします。



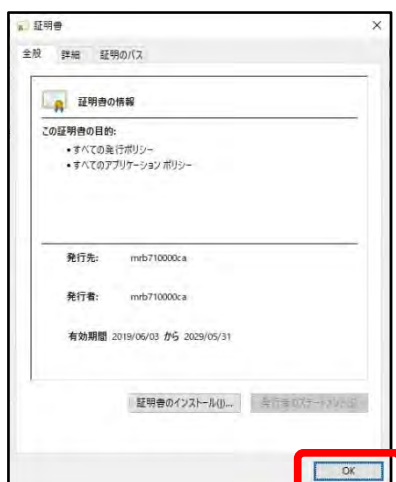
⑥内容を確認し、正しければ『完了』をクリックします。



④左のような警告が表示されますが、『はい』をクリックします。



⑦左のようなポップアップが表示されましたら『OK』をクリックします。



⑧『OK』をクリックして証明書のインポート作業は完了です。

その他の項目

・その他の項目 目次

1	グループ設定	P. 80
2	ログ閲覧	P. 83

1, グループ設定

グループ分けすることで、利用者や部署毎にセキュリティレベルを設定変更が可能になります。



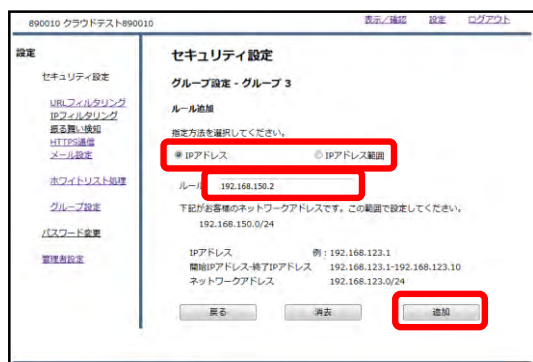
①管理画面にログイン後、右上の『設定』をクリックし、左側の『グループ設定』をクリックします。



②設定するグループを選択し、『編集』をクリックします。



③『追加』をクリックします。



④所属させたいIPアドレスかIPアドレス範囲を選択し、ルールを記入し『追加』をクリックします。



⑤入力したルールを確認し、正しければ『追加』をクリックします。



⑥グループに対するセキュリティ設定をします。
手順は『セキュリティ設定』の章をご確認下さい。

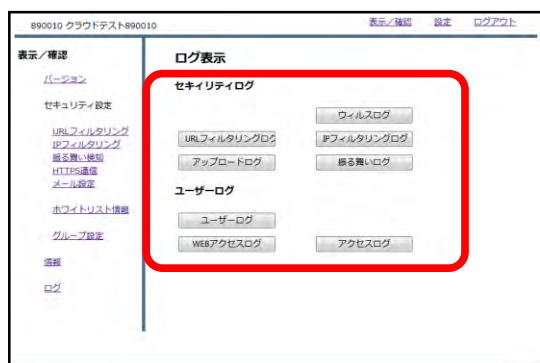
2, ログ閲覧

閲覧できるログの確認

MRBで検閲した通信のログを閲覧することができます。



①管理画面にログイン後、
左側の『ログ』をクリックします。



②各ボタンをクリックすることでそれ
ぞれのログを閲覧することができます。

③各ログの内容については以下のとおりです。

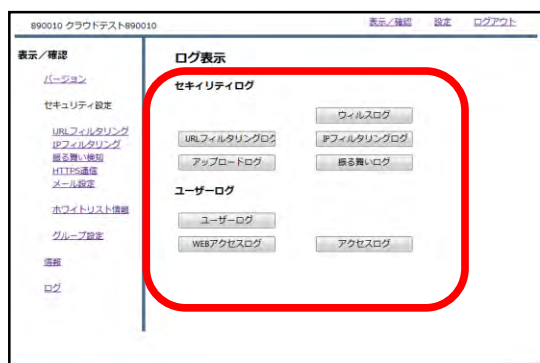
- | | |
|----------------|--|
| ・ ウィルスログ | ...ダウンロードしたデータがウイルスだった場合に記録されます |
| ・ URLフィルタリングログ | ...WEB閲覧時、URLフィルタリングにて通信をブロックした場合に記録されます |
| ・ IPフィルタリングログ | ...WEB閲覧時、IPフィルタリングにて通信をブロックした場合に記録されます |
| ・ アップロードログ | ...データを外部にアップロードした際に記録されます |
| ・ 振る舞いログ | ...WEBサイト以外からの通信をブロックした際に記録されます |
| ・ ユーザーログ | ...ユーザがMRB管理画面にて行った操作が記録されます |
| ・ WEBアクセスログ | ...アクセスしたWEBサイトが記録されます |
| ・ アクセスログ | ...WEBサイト以外のアクセスが記録されます |

ログ閲覧時の操作

MRBで検閲した通信のログを閲覧を確認する際の操作です。



①管理画面にログイン後、
左側の『ログ』をクリックします。



②閲覧したいログのボタンをクリック
します。



③クリックしたボタンに対応するログ
が表示されます。
また、『ダウンロード』をクリック
することで、現在閲覧している最大300
件分のログデータをテキスト形式でダ
ウンロードすることができます。

④閲覧ログの操作は以下のとおりです。

The screenshot shows a log viewing interface with the following elements and callouts:

- ①: A box containing the text "1-100/1745 件".
- ②: A button labeled "ページ指定" followed by a text input field containing the number "1".
- ③: A button labeled "一覧に戻る".
- ④: A box containing the text "1/18 ページ".
- ⑤: Two buttons labeled "前のページ" and "次のページ".
- ⑥: A box containing the date "2019/08/20".
- ⑦: Three buttons labeled "最新のログ", "前日のログ", and "後日のログ".
- ⑧: A button labeled "ダウンロード".

- ①...現在閲覧しているログ番号/すべてのログ件数です
②...1ページあたり300件ごとに閲覧するログを指定できます
③...ログ一覧に戻ります
④...現在閲覧しているログページ/すべてのログページです
⑤...ログページの遷移ができます
⑥...閲覧しているログの日付です
⑦...閲覧するログの日付を変更できます
[最新のログ]は本日のログです
⑧閲覧しているログをテキスト形式でダウンロードすることができます