（Bizbox_SSB_v2.2版） 2023年4月13日改定

Security BOSS®
ゲートウェイ・セキュリティ運用監視サービス

ご利用の手引き

NTT PC COMMUNICATIONS

～ 目次 ～

1.『ご利用の手引き』のご案内

この度は、株式会社エヌ・ティ・ティピー・シーコミュニケーションズ（以下、「当社」といいます）Security BOSSシリーズ ゲートウェイ・セキュリティ運用監視サービス（以下、「サービス」といいます）をご利用いただき、まことにありがとうございます。

本書では、お客さまにサービスをご利用いただく際の手順、設定、各種お問い合わせについて、ご説明いたします。ご必要の際に参照できるよう、本書は大切に保管してください。また、サービスのご利用に伴う各種手続き、お問い合わせの際は本書を必ずお読みいただき、注意事項をお守りくださいますようお願いいたします。

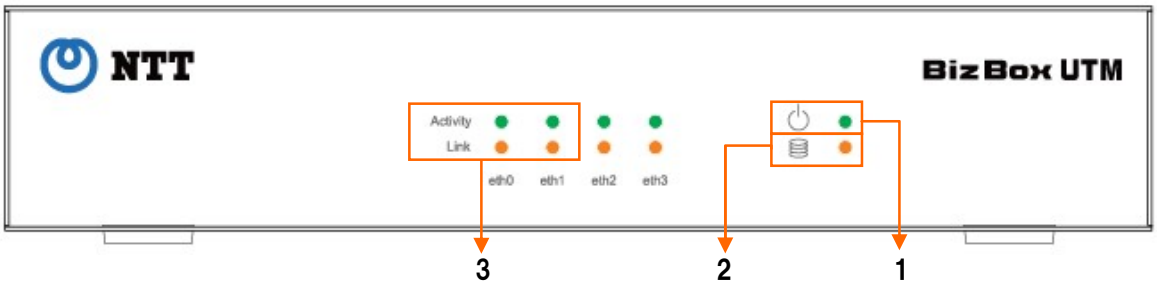
本サービスの概要や提供条件につきましては、別途、『ゲートウェイ・セキュリティ運用監視サービス 仕様書』をご覧ください。なお、本サービスにおきましては、当社への各種お問い合わせ・連絡先と致しまして、NTTPCセキュリティ・オペレーション・センタ（以下、「SOC【ソック】」といいます）が一元的に受け付けております。
巻末に記載されてあります連絡先へご連絡ください。

2. ハードウェアについて

2－1 ゲートウェイ装置各部の説明

ゲートウェイ装置の主要な操作部、確認部分を下記に示します。

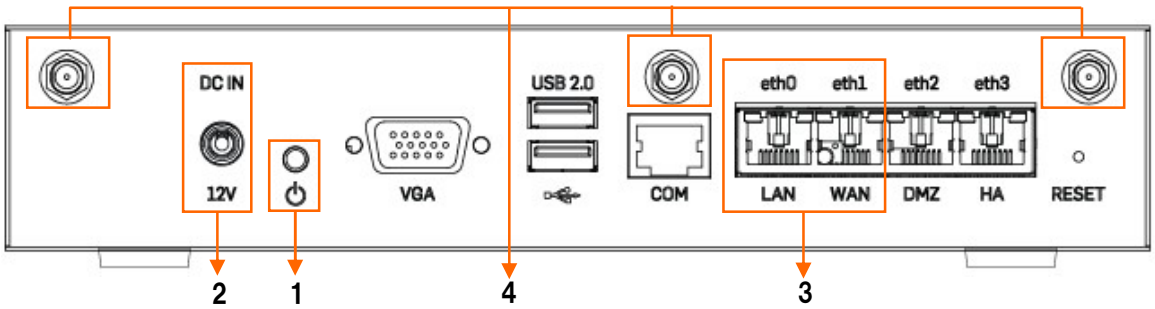
■ Biz Box UTM「SSB」「5」（ライト・オンデマンド・ネクストプラン）



図：2-1-1 Biz Box UTM「SSB」「5」前面部

	LED ランプの名称等		表示（色）		状態
1	⏻	電源ランプ	青	点灯	電源が入っている状態です。
				消灯	電源が切れている状態です。
2	≡	SSD アクセスランプ	橙	点灯	SSD が動作状態です。
				消灯	SSD が動作していない状態です。
3	eht0 / eth1	イーサポートアクティビティランプ（上段）	緑	点灯	イーサポートが通信状態です。
				消灯	イーサポートが通信していない状態です。
		イーサポートリンクランプ（下段）	橙	点灯	イーサポートのリンクがアップ状態です。
				消灯	イーサポートのリンクがダウン状態です。

※説明のないLEDランプは未使用です。



図：2-1-2 Biz Box UTM「SSB」「5」背面部

	名称	状態
1	⏻	電源スイッチ
2	DC IN	電源ケーブル差込口
3	eth0 ～ eth1	イーサネットポート
4	WiFi アンテナコネクタ	WiFi アンテナ接続用コネクタ

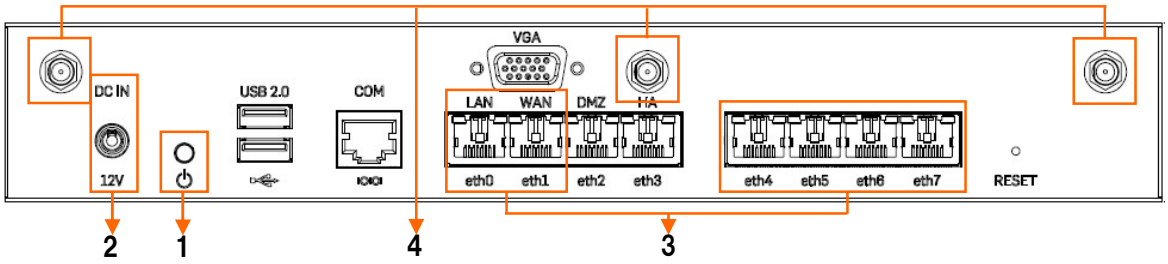
※説明のないポートは未使用です。

■ Biz Box UTM「SSB」「Standard／Professional」（ライト・オンデマンド・ネクストプラン）

図：2-1-3 Biz Box UTM「SSB」「Standard／Professional」前面部

	ランプの名称等		表示（色）		状態
1	⏻	電源ランプ	青	点灯	電源が入っている状態です。
				消灯	電源が切れている状態です。
2	≡	SSD アクセスランプ	橙	点灯	SSD にアクセスしている状態です。
				消灯	SSD にアクセスしていない状態です。
3	eth0 / eth1 /eth4 / eth5 / eth6 / eth7	イーサポートアクティビティランプ（上段）	緑	点灯	イーサポートが通信状態です。
				消灯	イーサポートが通信していない状態です。
		イーサポートリンクランプ（下段）	橙	点灯	イーサポートのリンクがアップ状態です。
				消灯	イーサポートのリンクがダウン状態です。

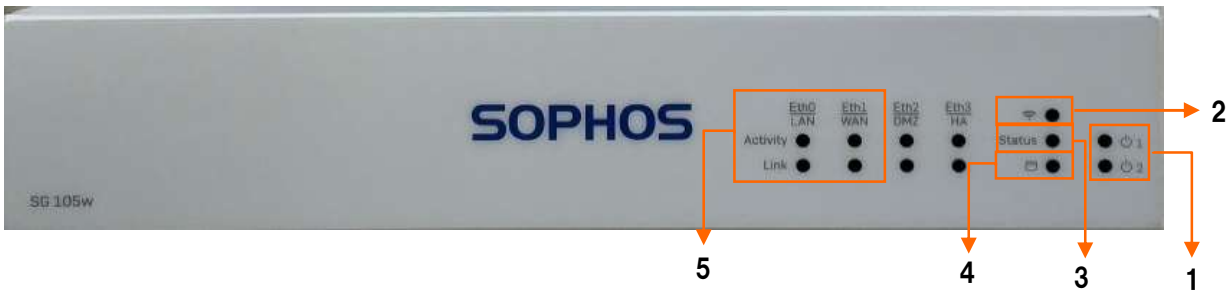
※説明のないLEDランプは未使用です。



図：2-1-4 Biz Box UTM「SSB」「Standard／Professional」背面部

	名称	状態
1	⏻	電源スイッチ
2	DC IN	電源ケーブル差込口
3	eth0/eth1/eth4/eth5/eth6/eth7	イーサネットポート
4	WiFi アンテナコネクタ	WiFi アンテナ接続用コネクタ

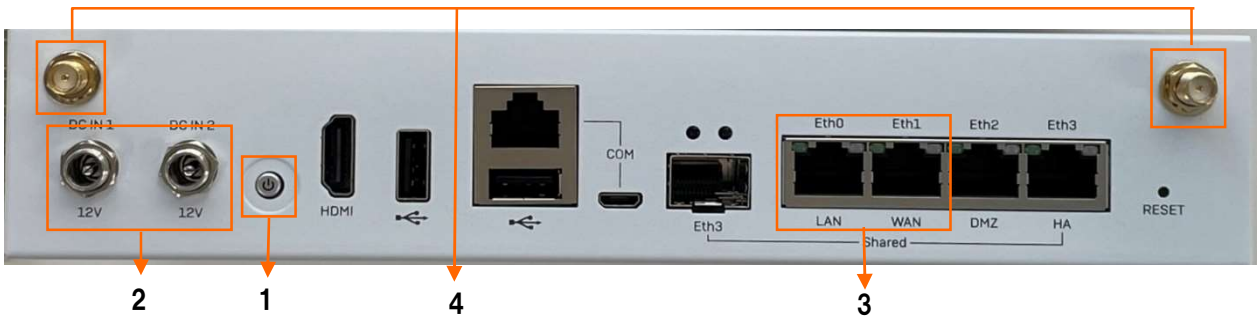
■Biz Box UTM「SG105w rev3」（ライト・オンデマンド・ネクストプラン）
（※「SG105w rev3」は「SSB」「5」の保守時の交換機器として使用されます。）



図：2-1-5 Biz Box UTM「SG105w rev3」前面部

	ランプの名称等		表示（色）		状態
1	⏻	電源ランプ	緑	点灯	電源が入っている状態です。
				消灯	電源が切れている状態です。
			赤	点灯	電源アダプタが失敗または切断している状態です。
2	Wi-Fi	Wi-Fi ランプ	緑	点灯	Wi-Fi が有効な状態です。
				消灯	Wi-Fi が無効な状態です。
3	Status	状態ランプ	緑	点灯	通常に作動中
				点滅	デバイスが起動中またはシャットダウン中の状態です。
			赤	点灯	SSD または起動の失敗の状態です。
				点滅	一般的なエラーの状態です。
4	⛁	SSD アクセスランプ	青	点滅	SSD ドライブが使用中です。
5	eth0 / eth1	イーサポートアクティビティランプ（上段）	緑	点灯	イーサポートが通信状態です。
				消灯	イーサポートが通信していない状態です。
		イーサポートリンクランプ（下段）	橙	点灯	イーサポートのリンクがアップ状態です。
				消灯	イーサポートのリンクがダウン状態です。

※説明のない LED ランプは未使用です。



図：2-1-6 Biz Box UTM「SG105w rev3」背面部

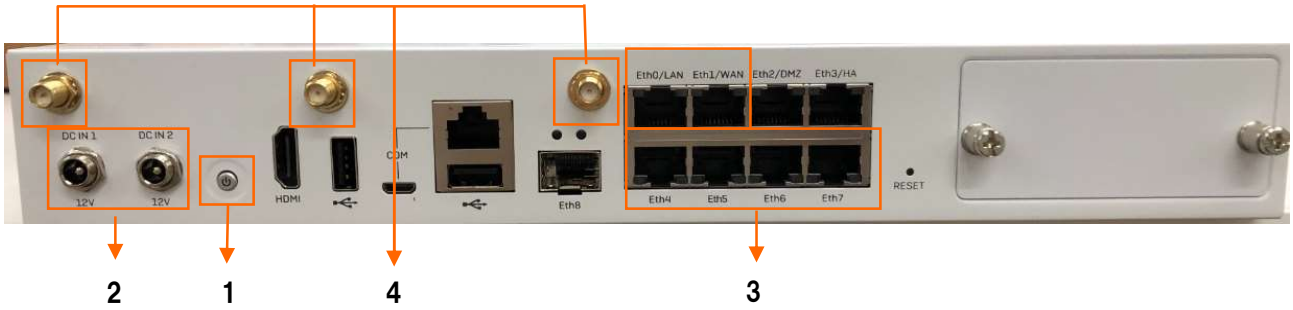
	名称	状態
1	⏻	電源スイッチ
2	DC IN	電源ケーブル差込口
3	eth0/eth1	イーサネットポート
4	WiFi アンテナコネクタ	WiFi アンテナ接続用コネクタ

■ Biz Box UTM「SG125w rev3」（ライト・オンデマンド・ネクストプラン）
（※「SG125w rev3」は「SSB」「Standard」の保守時の交換機器として使用されます。）

図：2-1-7 Biz Box UTM「SG125w rev3」前面部

	ランプの名称等		表示（色）		状態
1	⏻	電源ランプ	緑	点灯	電源が入っている状態です。
				消灯	電源が切れている状態です。
			赤	点灯	電源アダプタが失敗または切断している状態です。
2	📶	Wi-Fi ランプ	緑	点灯	Wi-Fi が有効な状態です。
				消灯	Wi-Fi が無効な状態です。
3	Status	状態ランプ	緑	点灯	通常に作動中
				点滅	デバイスが起動中またはシャットダウン中の状態です。
			赤	点灯	SSD または起動の失敗の状態です。
				点滅	一般的なエラーの状態です。
4	🛢	SSD アクセスランプ	青	点灯	SSD ドライブが使用中です。
5	eth0 / eth1 /eth4 / eth5 / eth6 / eth7	イーサポートアクティビティランプ（上段）	緑	点灯	イーサポートが通信状態です。
				消灯	イーサポートが通信していない状態です。
		イーサポートリンクランプ（下段）	橙	点灯	イーサポートのリンクがアップ状態です。
				消灯	イーサポートのリンクがダウン状態です。

※説明のない LED ランプは未使用です。



図：2-1-8 Biz Box UTM「SG125w rev3」背面部

	名称	状態
1	⏻	電源スイッチ
2	DC IN	電源ケーブル差込口
3	eth0/eth1/eth4/eth5/eth6/eth7	イーサネットポート
4	WiFi アンテナコネクタ	WiFi アンテナ接続用コネクタ

2－2 装置諸元

サービスタイプ		ライト・オンデマンド・ネクスト			
使用機器		Biz Box UTM「SSB」「5」	Biz Box UTM「SSB」「Standard」 Biz Box UTM「SSB」「Professional」	Biz Box UTM「SG105w rev3」	Biz Box UTM「SG125w rev3」
外形仕様	形状	デスクトップ（ラックマウント不可）			
	本体寸法（W）×（H）×（D）	225×44×150（mm）	28×44×186.8（mm）	225×44×150（mm）	305×44×205（mm）
	質量	1.19kg	1.70kg	1.11kg	1.80kg
電源仕様	電源数	1口		2口	
	ケーブル長	1500mm（ACアダプタ側）※ACアダプタ除く 1830mm（電源プラグ側）		1800mm	
	電源形状	2極プラグ			
	入力電圧	AC入力 100V-240V			
	入力電流	3.3A以下	3.0A 以下	1.5A 以下	3.0A 以下
	周波数	50Hz/60Hz			
	消費電力	4.83W/9.84W（スタンバイ/フル）	12.46W/26.16W（スタンバイ/フル）	8.88W/10.44W（スタンバイ/フル）	18.6W/20.04W（スタンバイ/フル）
環境動作仕様	動作温度	0℃ - 40℃			
	保管温度	-20℃ - 80℃			
	保管湿度	10% - 90%（結露なきこと）			

※ 装置諸元は予告なしに変更される場合がございます。

3. 導入の準備

本サービスはお客さま宅内に設置したゲートウェイ装置によって提供いたします。
ゲートウェイ装置の設置工事前に、お客さま宅内での設置準備をお願いいたします。

3－1 ゲートウェイ装置の設置準備

『2－2 装置諸元』を確認し、以下の項目について設置準備をおこなってください。
ゲートウェイ装置の設置工事当日は、以下の結果を工事担当者にお伝えください。

［手順1］設置場所の確保
『外形仕様』、『環境動作仕様』を確認し、設置する場所を確保してください。

［手順2］ゲートウェイ装置が使用する電源の確保
電源要件を確認し、電源の確保をおこなってください。

［手順3］対向機器の状態確認
対向機器の設置場所、接続先ポート番号を確認してください。

［手順4］物品の準備
ゲートウェイ装置を対向機器と接続するためのイーサネットケーブル（LAN ケーブル）は、原則お客さま準備となります。
また、ゲートウェイ装置から電源までの距離が遠い場合は、延長用の電源ケーブルの準備もお願いいたします。

3－2 エンドユーザマニュアルの配布

ゲートウェイ装置の設置工事前までに、エンドユーザの方へ『エンドユーザマニュアル』を配布してください。

メールアンチスパム・アンチウィルスを使用するお客さまの場合、工事前にエンドユーザの方に設定していただく項目があります。設定方法は『エンドユーザマニュアル』に記載されておりますので、工事前に必ずおこなっていただけますようお願いいたします。

（注）Biz Box UTM「SSB」「5」、「SG105 rev3」の場合は設定不要です。

① HTMLメールの受信設定

隔離されたメールのリスト（隔離レポート）（『4－3 隔離レポート』 参照）は、ゲートウェイ装置からHTML形式のメールにて送信されます。
このため、エンドユーザの方がお使いのメールソフトにて、HTMLメールを受信できるように設定していただく必要がございます。

② サーバからメッセージのコピーの削除

ゲートウェイ装置の設置工事の際、メールサーバに大量のEメールが残っていますと、ゲートウェイ装置に大量の負荷がかかり、工事が失敗してしまう恐れがあります。
このため、エンドユーザの方がご使用のメールソフトにて、メールサーバからEメールのコピーを削除する設定をおこなっていただく必要がございます。
※工事後は設定を戻していただいてかまいません。

③ APOPの無効化

ゲートウェイ装置は、メールソフトからのEメール受信の際に、APOPは対応しておりません。
このため、エンドユーザの方がご使用のメールソフトにて、APOPを無効にしていただく必要がございます。
また、ゲートウェイ装置がメールサーバに対してEメール受信を行う場合も、ゲートウェイ装置はAPOPに対応しておりませんので、メールサーバ上でもAPOPを無効にしていただく必要がございます。

3－3 工事当日の立会い

工事当日には、設置工事担当者が参りますので、対応をお願いいたします。また、事前に確認していただいた以下の情報や物品を、工事担当者にお渡ししていただくようお願いいたします。

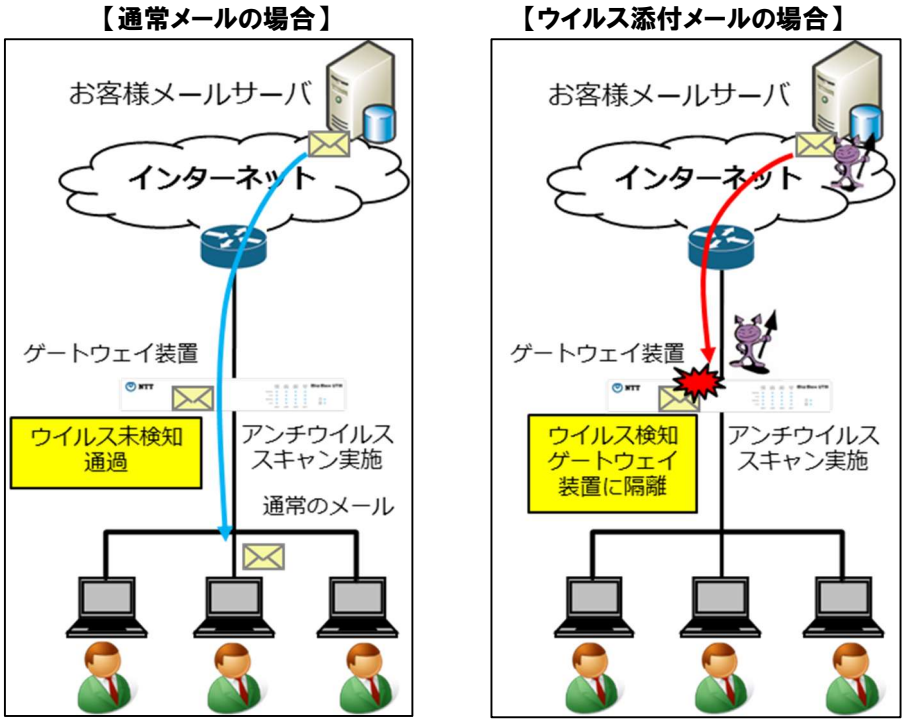
① ゲートウェイ装置の設置場所
② 対向装置の場所・ポート番号
③ 必要に応じてお客さまに準備していただいた物品（イーサネットケーブル、延長用電源ケーブルなど）

4. 運用方法

この項目では、サービスにおける全ての機能を記載しております。ご契約内容を確認していただき、ご利用されているサービス項目についてお読みいただきますようお願いいたします。
サービス内容の詳細については、仕様書をご確認ください。

4－1 メールアンチウイルス

SMTPやPOP3で送受信されるEメールや添付ファイルに、ウィルスが含まれていないかスキャンをおこないます。ウィルスが検知された場合、ゲートウェイ装置内にそのEメールを隔離します。ウィルスが検知されず、またスパムメールでもないと判定されたEメールは、通常通りに送信されます。



図：4-1-1 メールアンチウイルス

隔離したEメールのリスト（以下、「隔離レポート」という）を、ゲートウェイ装置からEメールの宛先である各アカウントへ、1日1回（最大1日2回）HTMLメールにて送信します。（『4－2 メールアンチスパム』が隔離設定の場合のみ）

（注）Biz Box UTM「SSB」「5」、「SG105 rev3」の場合には隔離レポートは利用できません。

隔離レポートでは、隔離されたEメールの詳細（日時、差出人、宛先、件名、理由（spam/virus）、サイズ）を確認できます。（『4-3 隔離レポート』 参照）

なお、ウィルスメールと判定された場合、改めて該当のEメールを受信（リリース）することはできません。操作手順については『エンドユーザマニュアル』をご確認ください。

４－１－１ 運用方法

ウィルスのスキャンは、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

４－１－２ ご注意事項

ウィルスと判断されたEメールは、リリースをおこなうことができません。ウィルスと判断されたEメールは有害であるため、改めて該当Eメールをゲートウェイ装置からリリースし、受信をおこなうことはできません。
その上で、ウィルスと判定されたEメールを確認したい場合は、受信された隔離レポートの内容を、SOCまでお知らせいただく必要がございます。

【メールサーバ上のEメールパスワード変更時は、メールソフト上のパスワードも併せて変更してください。】

メールサーバ上でEメールのパスワードを変更した場合は、メールソフト上のパスワードも併せて変更してください。メールソフト上のパスワードを変更せずにメールの受信をおこないますと、約20分間は、ゲートウェイ装置が変更前のパスワードを使用して、メールサーバにEメールを受信しようとします。この間、エンドユーザのメールソフト上では、何もエラーメッセージは表示されません。約20分後、ゲートウェイ装置が保持していた変更前のパスワードを消去した後、エンドユーザがメールサーバでEメールの受信をおこないますと、パスワード認証エラーのメッセージがメールソフト上で表示されます。

【Eメールの受信には、最大で5分ほど時間がかかる場合があります。メールサーバ上のEメールパスワード変更時は、メールソフト上のパスワードも併せて変更してください。】

メールアンチスパム（『４－２　メールアンチスパム』 参照）で、スパムメール検知時の処理を隔離に設定した場合、ゲートウェイ装置が定期的にメールサーバよりEメールを受信し、スキャンをおこないます。このため、送信から受信までに最大で5分程時間がかかります。なお、ゲートウェイ装置が定期的に受信をおこなうメールサーバは、あらかじめ装置に登録されたサーバのみとなります。

【モバイル端末でのEメールの受信は、不具合が生じる場合があります。】

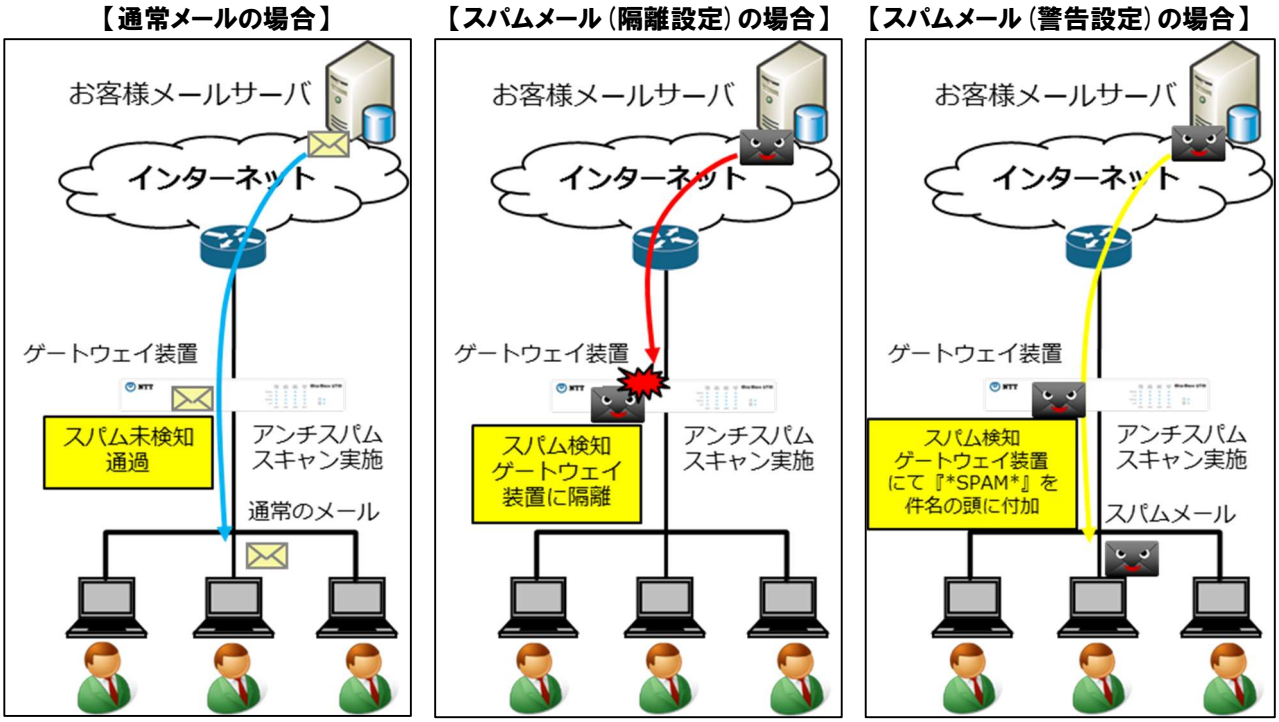
ゲートウェイ装置配下あてのEメールをモバイル端末で受信する場合は、Eメールの配信に不具合が生じる場合があります。モバイル端末でEメールを受信する場合には、サーバにEメールを残す設定をおこなった上で受信をおこなってください。

4－2 メールアンチスパム

(注) Biz Box UTM「SSB」「5」、「SG105 rev3」の場合メールアンチスパム機能は利用できません。

SMTPやPOP3で受信されるEメールや添付ファイルが、スパムメールに該当しないかスキャンをおこないます。スパムが検知された場合、ゲートウェイ装置は以下のどちらかの処理をおこないます。

・隔離 → ゲートウェイ装置内にEメールを隔離
・警告 → Eメールの件名の頭に『*SPAM*』を付加し、宛先へ送信スパムと判定されず、またウィルスも検知されなかったEメールは、通常通りに送信されます。



図：4-2-1 メールアンチスパム

隔離したEメールの1日分のリスト（隔離レポート）を、ゲートウェイ装置からEメールの宛先である各アカウントへ、HTMLメールにて送信します。
隔離レポートでは、隔離されたEメールの詳細（送信日時、送信元、宛先、件名、隔離された理由（spam/virus）、サイズ）を確認できます。（『4-3 隔離レポート』 参照）
ゲートウェイ装置から取り出したいEメールがある場合は、リリースをおこなってください。操作手順については『エンドユーザマニュアル』をご確認ください。

※隔離されたスパムメールにはフィッシング詐欺も含まれます。リリースしたEメールのURLは安易にブラウザなどで表示させないでください。

4－2－1 運用方法

スパムのスキャンは、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

４－２－２ ご注意事項

【メールサーバ上のEメールパスワード変更時は、メールソフト上のパスワードも併せて変更してください。】

メールソフト上のパスワードを変更せずにメールの受信をおこないますと、約20分間は、ゲートウェイ装置が変更前のパスワードを使用して、メールサーバにEメールを受信しようとします。この間、エンドユーザのメールソフト上では、何もエラーメッセージは表示されません。約20分後、ゲートウェイ装置が保持していた変更前のパスワードを消去した後、エンドユーザがメールサーバでEメールの受信をおこないますと、パスワード認証エラーのメッセージがメールソフト上で表示されます。

【Eメールの受信には、最大で5分ほど時間がかかる場合があります。】

スパムメール検知時の処理を隔離に設定した場合、ゲートウェイ装置が定期的にメールサーバよりEメールを受信し、スキャンをおこないます。このため、送信から受信までに最大で5分程時間がかかります。なお、ゲートウェイ装置が定期的に受信をおこなうメールサーバは、あらかじめ装置に登録されたサーバのみとなります。

【モバイル端末でのEメールの受信は、不具合が生じる場合があります。】

ゲートウェイ装置配下あてのEメールをモバイル端末で受信する場合は、Eメールの配信に不具合が生じる場合があります。モバイル端末でEメールを受信する場合には、サーバにEメールを残す設定をおこなった上で受信をおこなってください。

４－２－３ こんな時は・・・

【通常のEメールが頻繁にスパムメールと判定されてしまう。】

⇒ 一箇所から大量のEメールを受信される場合（メーリングリスト、社内アカウント、取引先）等は、スパムメールとして検知される可能性があります。通常のEメールが頻繁にスパムメールと判定されてしまう場合は、お客さまにてゲートウェイ装置の『メール送信者ホワイトリスト』に当該メールアドレス登録することでスパム判定対象外とすることが可能です。詳細は『４－９ メール送信者ホワイトリスト設定』をご参照ください。

【スパムメールと判断されたEメールのリリースができない。】

⇒ ①過去に1度リリースをおこなっている可能性があります。1度リリースをおこなったメールの再リリースはおこなえません。

⇒ ②すでにゲートウェイ装置から削除されている可能性があります。隔離されたEメールは16日後には削除されます。スパムメールと誤検知されてしまったEメールは、16日以内にリリースしてください。

【スパムメールを隔離せず通常のメールと同様受信したい。】

⇒ スパム判定されたEメールを隔離せず、件名の先頭に『＊SPAM＊』が付与される形で通常のEメールと同様に受信したい場合は、変更サービスオーダシートのPOP3メールスキャン設定を『隔離』から『警告』に変更し、SOCまで設定変更依頼をおこなってください。（『５ ユーザ・サポート・サイト』 参照）

4－3 隔離レポート(Quarantine Report)

(注)隔離レポート機能はBiz Box UTM「SSB」「5」、「SG105 rev3」では利用できません。

メールアンチスパム・アンチウィルスでスパムメールやウィルスメールと判定され、ゲートウェイ装置内に隔離されたEメールのリストは、隔離レポートとして、ゲートウェイ装置から送信されます。

隔離されたEメールは、1日1回(1日のうち午前1時以降のメール初回受信後)ゲートウェイ装置内で集計され、その結果をもとに隔離レポートが作成されます。作成された隔離レポートは、Eメールのあて先である各アカウントに、HTMLメールにて送信されます。

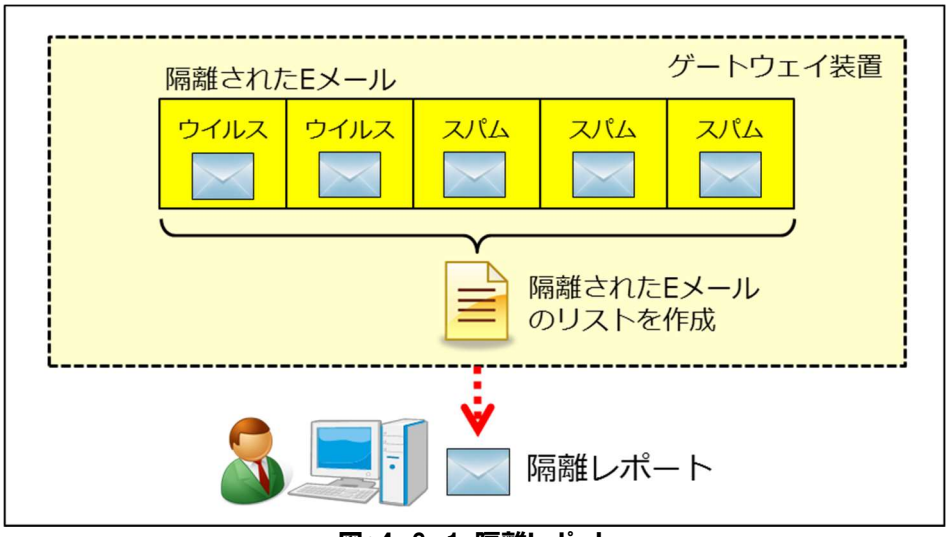


図:4-3-1 隔離レポート


SOPHOS Quarantine Report

Security BOSS®

このレポートは隔離されたメールの一覧です。
これらのメールはスパム、ウイルス、配信エラー といった理由で送信を止められています。
ご質問はシステム管理者宛にご連絡ください。

なお、このメールは送信専用のため、返信しないようお願いします。

前回の通知以降に隔離されたメール:

日時	差出人	宛先	件名	理由	サイズ	アクション
2013-10-21 18:03	mailmag@mag2.com	sasaki_1029@yahoo.co.jp	ムダな努力をしている人へ、(今日まで)	spam	7KB	リリース
2013-10-21 18:03	magchekimax@mag2.com	sasaki_1029@yahoo.co.jp	経産婦を自宅で出産するための方法はコレ!／骨中のゾクゾク感が止まらない!経営者にから届く恐怖の怪談メール..いま、読者増加中の人気クレンネルマガをご紹介ほぐ チェキMAK!]	spam	26KB	リリース
2013-10-21 18:03	naruhodoR@mag2.com	sasaki_1029@yahoo.co.jp	42才女が注・無添加ジュースを飲んだら、／停電してもPC仕事ができる!?「isologue」磯崎さんの徹底した災害対策【なるほどまぐ R】	spam	32KB	リリース
2013-10-21 18:03	magpremium@mag2.com	sasaki_1029@yahoo.co.jp	すごっ、60kgの私が!?／ジブリ幼稚園がアニメとしては一番しっくりくると痛感、松尾スズキが語る「ジブリ特品」会読者増加へつながるぁぇ見せ!【ちぇ見せまぐ!】	spam	30KB	リリース
2013-10-21 18:03	mailmag@mag2.com	sasaki_1029@yahoo.co.jp	【先着】あと23人です。	spam	7KB	リリース
2013-10-21 18:03	kabumag@mag2.com	sasaki_1029@yahoo.co.jp	5年以上買い続けたFX設定法(限定無料)／東京オリンピック関連の銘柄は今が買い!?北浜流一郎氏が買い時を分析!【株のまぐまぐ!】	spam	29KB	リリース
2013-10-21 18:04	entamag@mag2.com	sasaki_1029@yahoo.co.jp	豪華賞品が抽選で当たる!CMモニター登録／激レア動画☆わんこVSにゃんこのリアルファ小をお届け!ジワジワくるポケてコーナーも【エンタまぐ!】	spam	27KB	リリース
2013-10-21 18:04	magchekimax@mag2.com	sasaki_1029@yahoo.co.jp	ユニクロギフトカード1万円分プレゼント!／外食のプロに合コン/韓国家がオススメするレストランを大公開会話題のメルマガ4誌をご紹介ほぐ チェキMAK!]	spam	25KB	リリース
2013-10-21 18:04	tremag@mag2.com	sasaki_1029@yahoo.co.jp	【トレまぐ!】美さん候補に即決定!男性が何気もかいいと思う女性の特徴ベスト3／美大切の違攻解決法を大公開!	spam	16KB	リリース
2013-10-21 18:04	naruhodoR@mag2.com	sasaki_1029@yahoo.co.jp	関西弁だけで異会話が身についた!!／防災の日!アイドル・吉野はるなさんがコレクションを守るためにやっているコトは?【なるほどまぐ R】	spam	34KB	リリース
2013-10-21 18:04	magnavi@mag2.com	sasaki_1029@yahoo.co.jp	CMモニター登録<無料>はこちらから!／ブラジルW杯では目を集めるのはどの選手か!?サッカーファン大満足のメルマガ5つ紹介【まぐ ナビ】	spam	39KB	リリース
2013-10-21 23:07	mailmag@mag2.com	sasaki_1029@yahoo.co.jp	【BBM:3500社153業界のデータ!】●会社四季報業界地図2014年版はビジネスブックマラソンvol.3380	spam	11KB	リリース

ンラインヘルプ:

ールをメールボックスに送って受信するには、リンク「リリース」をクリックしてください。

リース が可能かどうかは隔離された理由によります。
不明な点などについては、システム管理ご担当者にご連絡ください。

図:4-3-2 隔離レポート見本

４－３－１ 運用方法

スパムメールと判定され、隔離されたEメールを受信したい場合は、リリースをおこなうことにより、ゲートウェイ装置から取り出すことができます。隔離レポートの内容やリリース方法については、『エンドユーザマニュアル』をご参照ください。

４－３－２ ご注意事項

【隔離されたEメールは、16日後にゲートウェイ装置から自動的に削除されます。】

隔離されたEメールは16日を過ぎますと、ゲートウェイ装置から自動的に削除されます。エンドユーザにて、隔離レポートを定期的に確認していただき、必要なEメールは必ず16日以内にリリースしてください。

【隔離されたEメールは、メールサーバから削除されます。】

ゲートウェイ装置は、Eメールを隔離した場合、メールサーバにある該当Eメールを削除いたします。メールサーバにコピーは残りません。

【不特定多数の方がゲートウェイ装置を経由してEメールを受信する場合には、POP3スキャン設定を『隔離』から『警告』に変更してください。】

隔離レポートを受信可能であるのは、ゲートウェイ装置にあらかじめご使用のメールサーバを登録したお客さまのみとなります。また、メールサーバを登録していないEメールもアンチスパム・アンチウィルスにより、スキャンの対象となります。そのため、不特定多数の方がゲートウェイ装置配下よりEメールを受信する場合、スパムを検知したEメールは、万が一そのEメールが誤判定されたものであってもリリースすることができません。

それらの問題を回避するためには、変更サービスオーダシートのPOP3メールスキャン設定を『隔離』から『警告』に変更し、SOCまで設定変更依頼をおこなってください。(『５　ユーザ・サポート・サイト』

４－３－３ こんな時は・・・

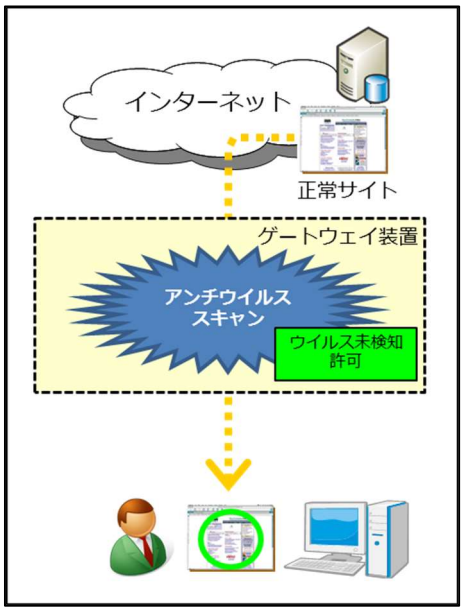
【HTMLメール未対応のメールソフトを使用したい場合。】

エンドユーザにて、HTML未対応のメールソフトを使用される場合、隔離レポートを閲覧することができないため、隔離メールをリリースすることができません。

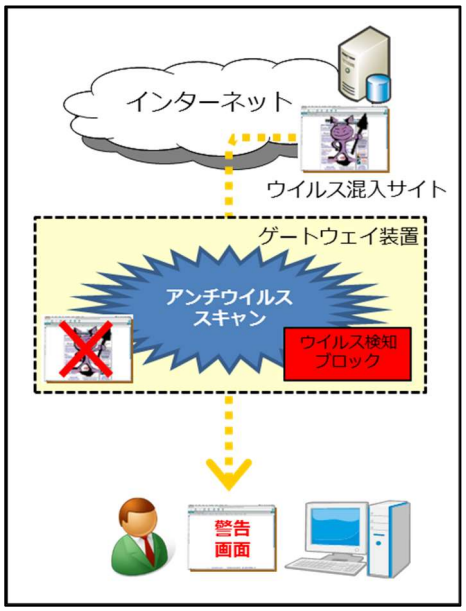
対処方法としましては、エンドユーザにてHTML対応のメールソフトに変更していただくか、もしくは、ゲートウェイ装置にてスパムメールメール検知時の処理を警告の設定にしていただき、メールソフト側でEメールのフィルタリングをしていただくことをおすすめします。

4－4 WEB アンチウィルス

エンドユーザがWEBサイトへのアクセスをおこなう際、そのWEBサイトに対して、ウィルスが含まれていないかスキャンをおこないます。ウィルスが含まれていると判定された場合、ゲートウェイ装置によってWEBアクセスをブロックし、警告画面を表示します。ウィルスが検知されなかった場合には、通常通りにWEBサイトが表示されます。



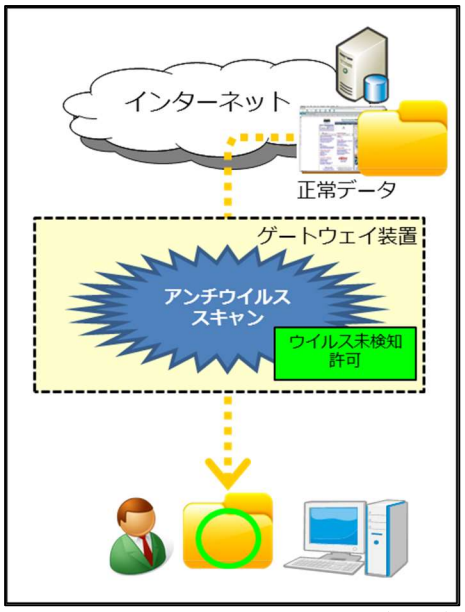
図：4-4-1 WEB アンチウイルス（通過）



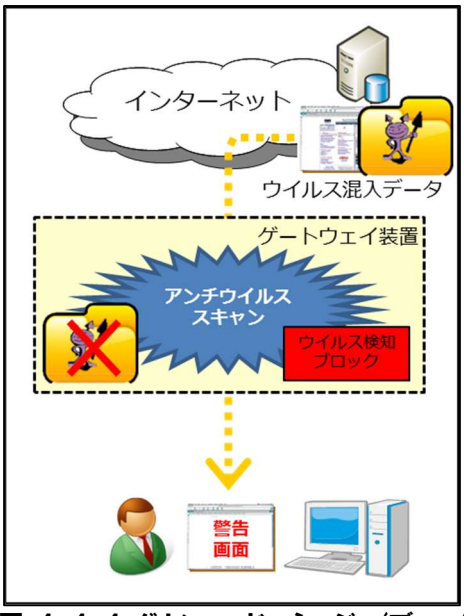
図：4-4-2 WEB アンチウイルス（ブロック）

WEBサイトなどからデータをダウンロードする際、データに対して、ウィルスのスキャンをおこないます。ウィルスが含まれていると判定された場合、ゲートウェイ装置によってデータのダウンロードをブロックし、警告画面を表示します。

ウィルスが検知されなかった場合には、通常通りにWEBサイトなどからデータをダウンロードできます。また、大きなデータなどでダウンロードに時間がかかってしまう場合には、ダウンロードマネージャが起動します。ダウンロードマネージャの操作方法は、『エンドユーザマニュアル』をご参照ください。



図：4-4-3 ダウンロードマネージャ（通過）



図：4-4-4 ダウンロードマネージャ（ブロック

４－４－１ 運用方法

WEBサイトのスキャンは、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

４－４－２ こんな時は・・・

【閲覧したいWEBサイトがブロックされてしまう。】

⇒ 業務などで閲覧したいWEBサイトがブロックされてしまう場合は、お客さまにてゲートウェイ装置にURLホワイトリストに当該URLを登録することによって、ブロック対象外とすることが可能です。詳細は『４－１０ URLカテゴリフィルタリング/URLホワイトリスト・ブラックリスト設定』をご参照ください。なお、ブロックされた理由によってSOCによる設定変更が必要となる場合もありますので、その際は変更サービスオーダシートのホワイトリストにWEBサイトのURLを記載し、SOCまで設定変更依頼をおこなってください。（『５ ユーザ・サポート・サイト』 参照）

４－４－３ HTTPS 通信のウイルスチェック方法

HTTPS通信に対してウイルスチェックをご利用になる場合、ゲートウェイ装置のHTTPSアンチウイルス設定を有効にする必要があります。また、クライアント端末へのCA証明書のインストールが必要になります。

（注）CA証明書がインストールできない端末ではご利用できません。

（注）ブラウザを使用しないアプリケーションやスマートフォン向けのアプリケーションなど、HTTPSアンチウイルスが有効の場合に、アプリケーションの仕様により通信できない場合があります。その場合にはHTTPSアンチウイルスを無効にしてください。

運用開始後にHTTPSウイルスチェックを有効にする場合には、変更サービスオーダシートに記載し、SOCまで設定変更依頼をおこなってください。（『５ ユーザ・サポート・サイト』 参照）

■CA証明書のインポート方法

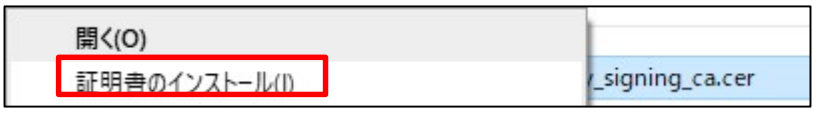
I

- ◆ 対応 OS： Windows10, 11
- ◆ 対応 Web ブラウザ： Microsoft Edge、Google Chrome、Firefox

Microsoft Edge、Google Chrome をご利用の場合のインポート手順

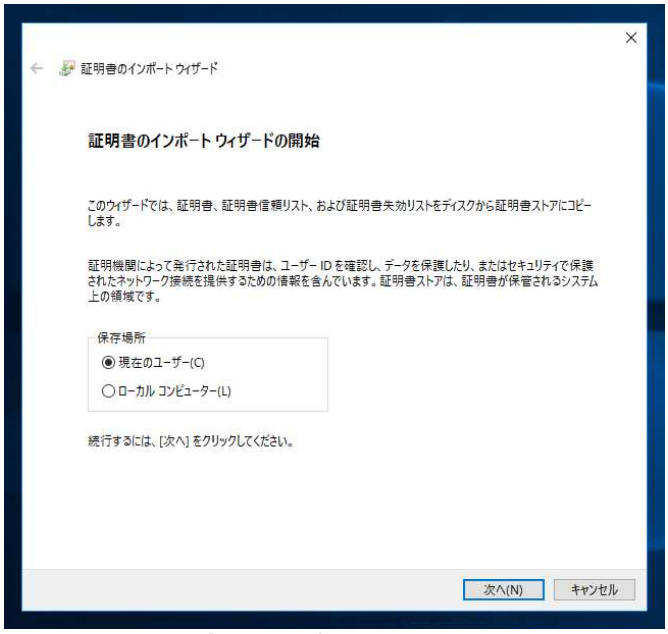
① CA 証明書の取得について窓口までお問合せください。窓口にて UTM から最新版の CA 証明書を取得し、お客様に送付させて頂きます。
② ご利用 PC の任意のフォルダに取得した CA 証明書ファイルを保存してください。

③ 証明書ファイルを右クリックし、「証明書のインストール」を選択します。



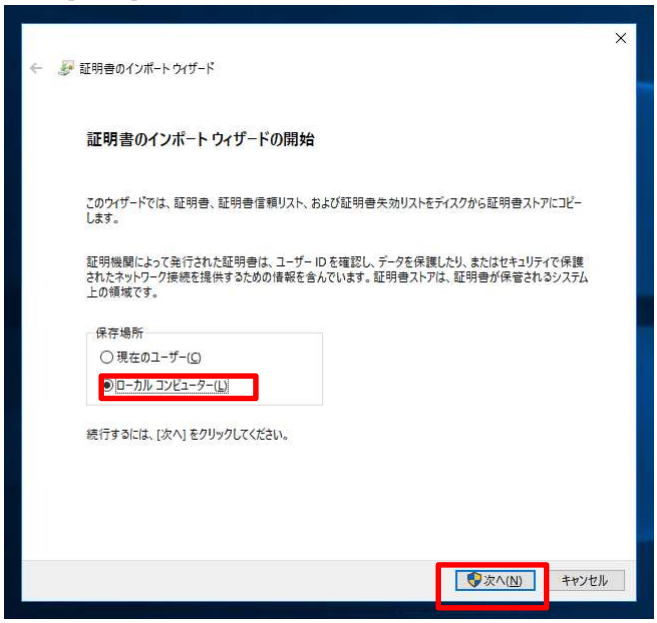
図：4-4-5 証明書を右クリック －「証明書のインストール」を選択

④ ［証明書のインポート ウィザードの開始］ダイアログが表示されます。



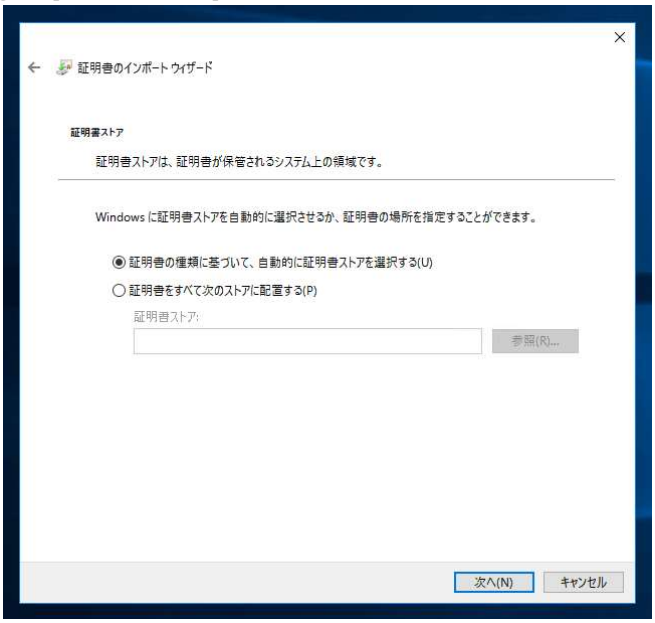
図：4-4-6 証明書のインポート ウィザードの開始

⑤　[保存場所] セクションで [ローカル　コンピューター] ラジオボタンをクリックしてチェックを付けます。チェック後 [次へ] ボタンをクリックします。



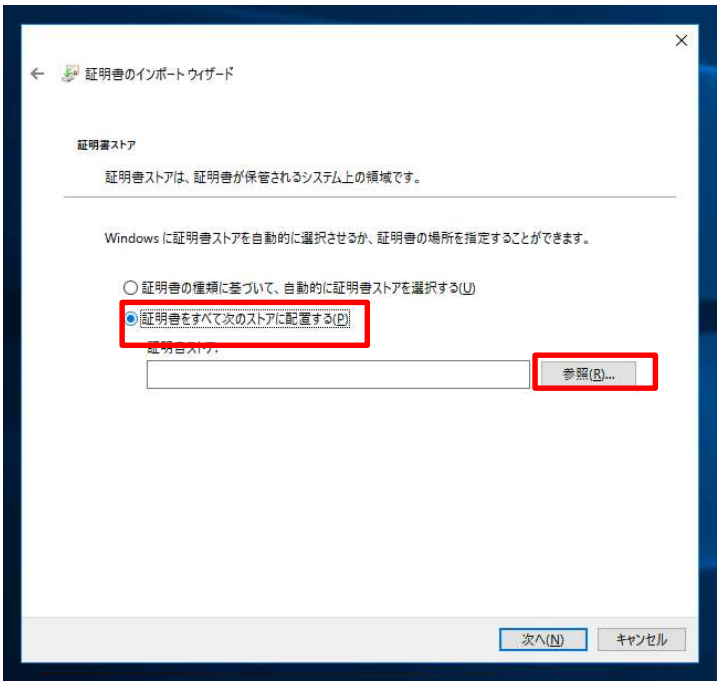
図：4-4-7 証明書のインポート ウィザード　証明書の保存場所

⑥　[証明書ストア] 画面が表示されます。



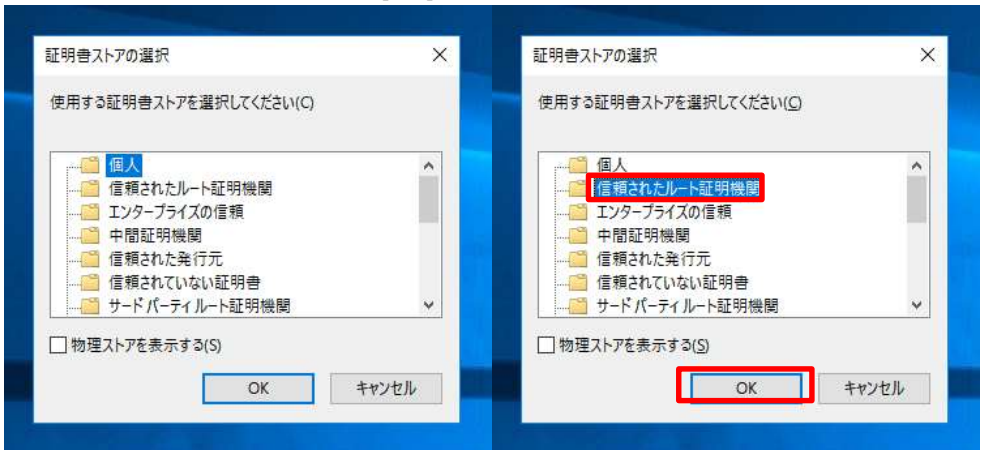
図：4-4-8 証明書のインポート ウィザード　証明書ストア

⑦ ［証明書をすべて次のストアに配置する］ラジオボタンをクリックしてチェックします。チェック後［参照］ボタンをクリックします。



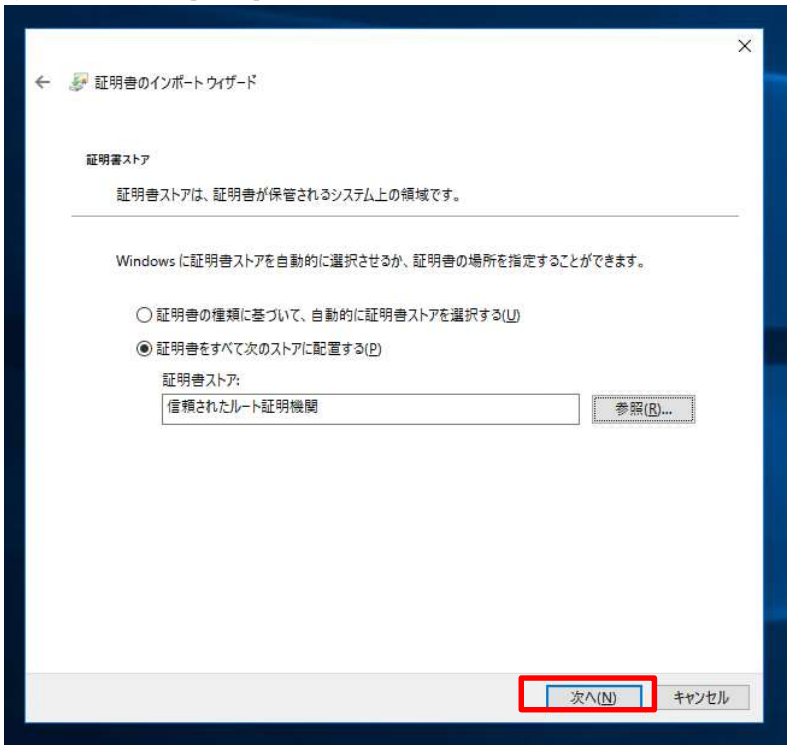
図：4-4-9 証明書ストア 「証明書をすべて次のストアに配置する」を選択し「参照」をクリック

⑧ ［証明書ストアの選択］ダイアログが表示されます。リストの中の［信頼されたルート証明機関］をクリックして選択します。選択後ダイアログの［OK］ボタンをクリックします。



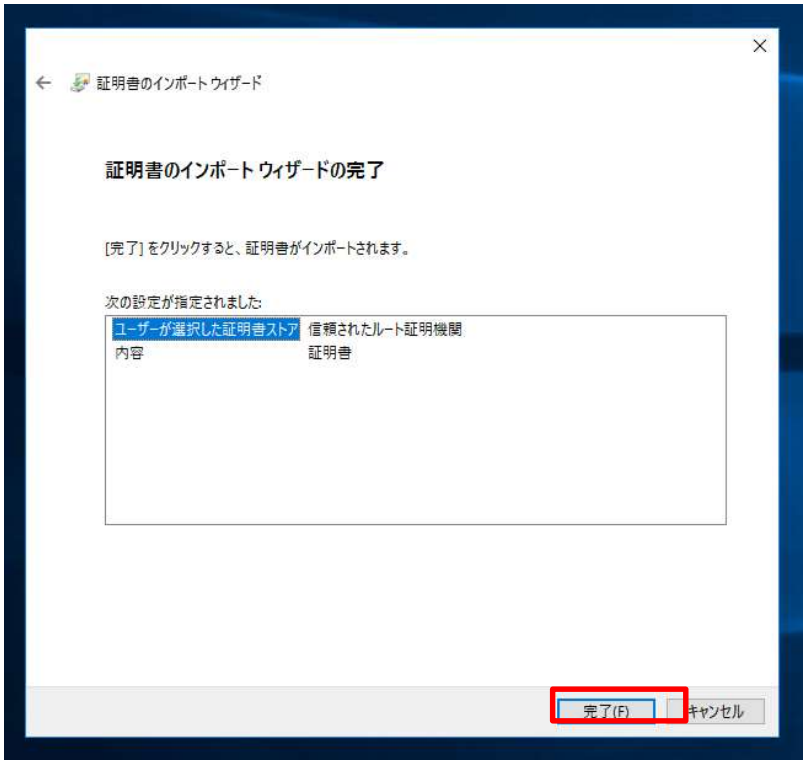
図：4-4-10 証明書ストアの選択

⑨ 設定ができたら［次へ］ボタンをクリックします。



図：4-4-11 証明書ストア「信頼されたルート証明機関」を選択した状態で「次へ」をクリック

⑩ ［証明書のインポート ウィザードの完了］ダイアログが表示されます。［完了］ボタンをクリックしてウィザードを終了します。



図：4-4-12 証明書のインポート ウィザードの完了

⑪ 「正しくインポートされました」と表示されます。「OK」をクリックします。

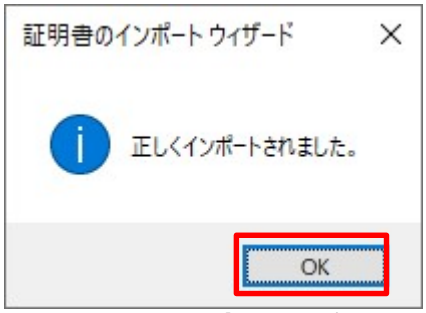


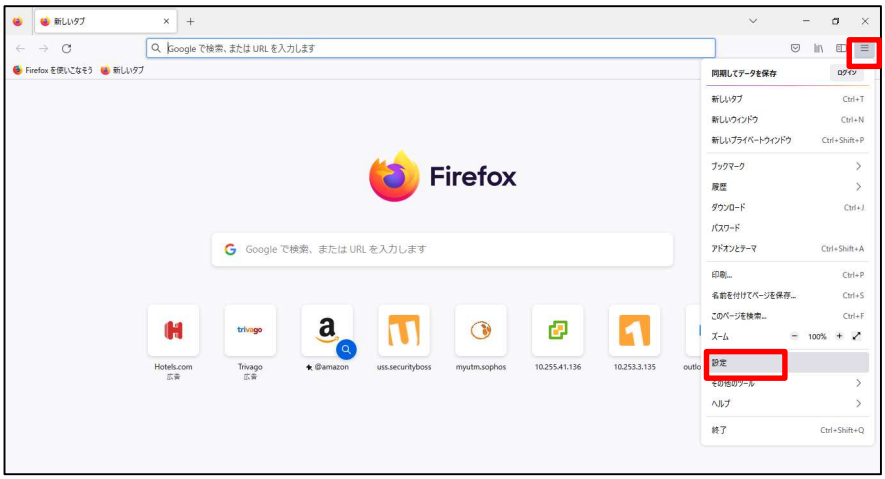
図:4-4-13 証明書のインポート 最終メッセージ

※もし、証明書インポート後に Microsft Edge, Google Chrome に「この接続ではプライバシーが保護されません」という表示が出てくる場合は、一度ブラウザを終了し、ブラウザを再度起動してインターネットへの接続をお試しください。

FireFox をご利用の場合のインポート手順

① CA 証明書の取得について窓口までお問合せください。窓口にて UTM から最新版の CA 証明書を取得し、お客様に送付させて頂きます。
② ご利用 PC の任意のフォルダに取得した CA 証明書ファイルを保存してください。

③ FireFox を起動し、右上の ☰ ボタンを押下し、「設定」をクリックします。

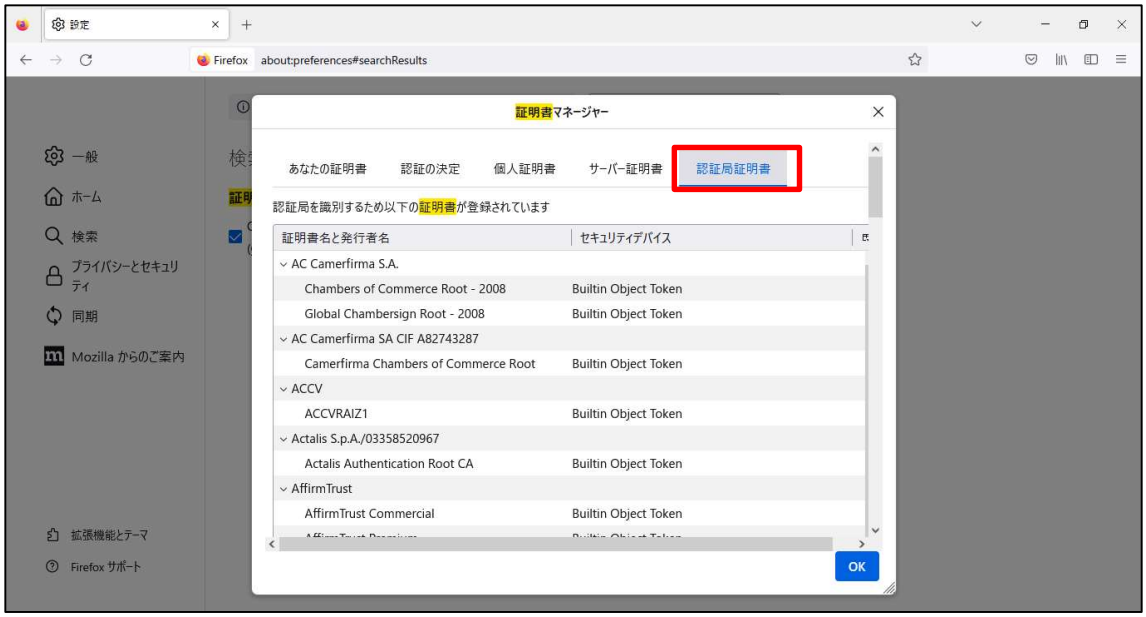


図：4-4-13 設定ボタンのクリック

④ 検索バーに「証明書」と入力します。「証明書を表示」のアイコンが表示されますので、クリックします。

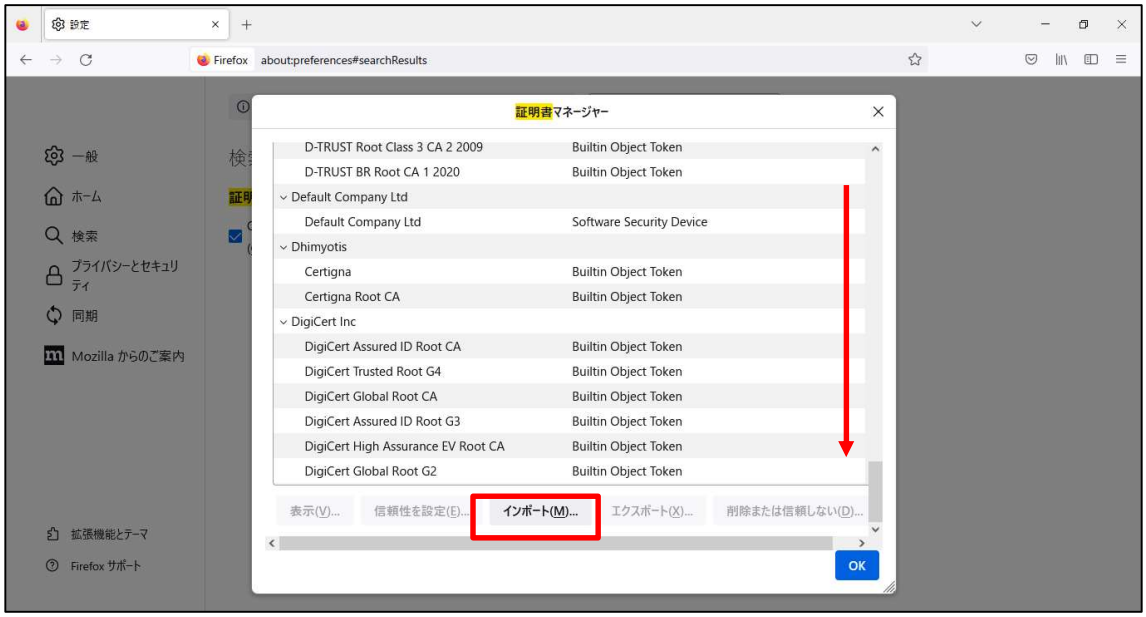
図：4-4-14 検索バーに「証明書」と入力後、「証明書を表示」をクリック

⑤　タブ「認証局証明書」をクリックします。



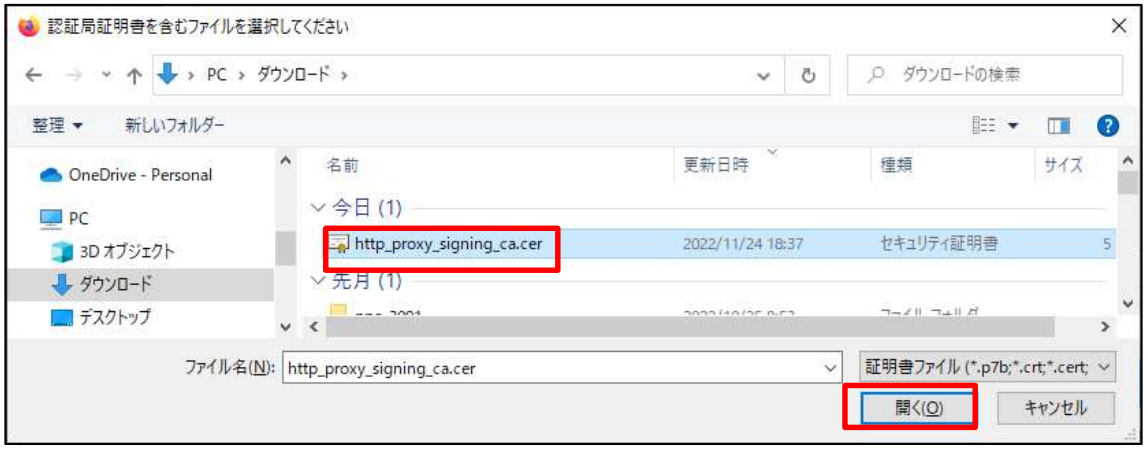
図：4-4-15　証明書マネージャー　「認証局証明書」を選択

⑥　一番下までスクロールし、「インポート」をクリックします。



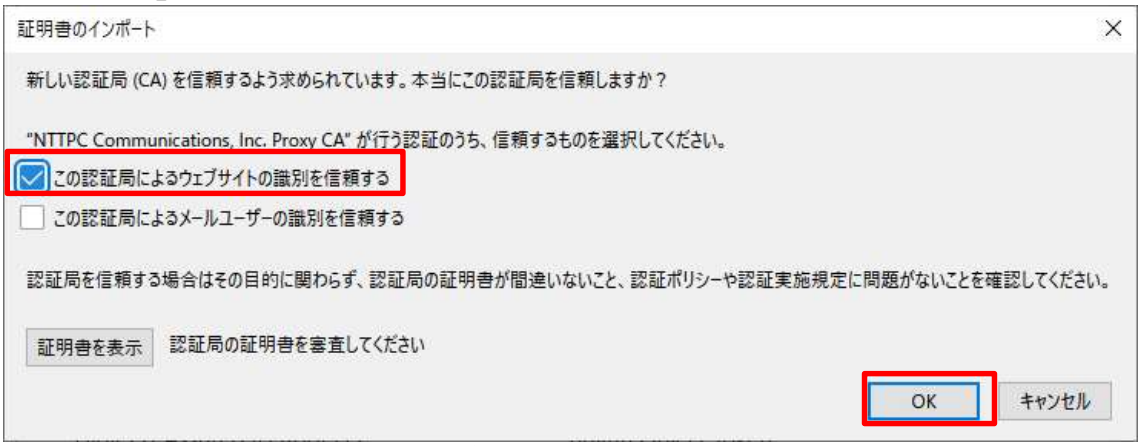
図：4-4-16　証明書マネージャー　「インポート」をクリック

⑦ 「認証局証明書を含むファイルを選択してください」が表示されますので、証明書ファイルを選択し、「開く」をクリックします。



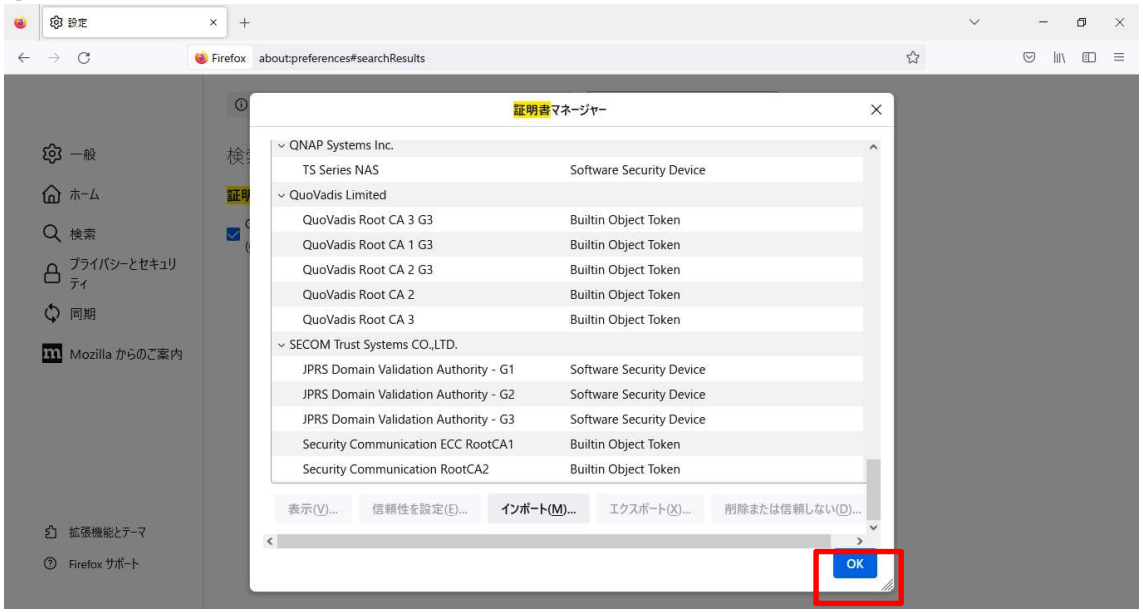
図：4-4-16 認証局証明書ファイルを選択

⑧ 「証明書のインポート」が表示されますので、「この認証局によるウエブサイトの識別を信頼する」にチェックを入れ、「OK」をクリックします。



図：4-4-17「この認証局によるウェブサイトの識別を信頼する」を選択

⑨ 「OK」をクリックします。

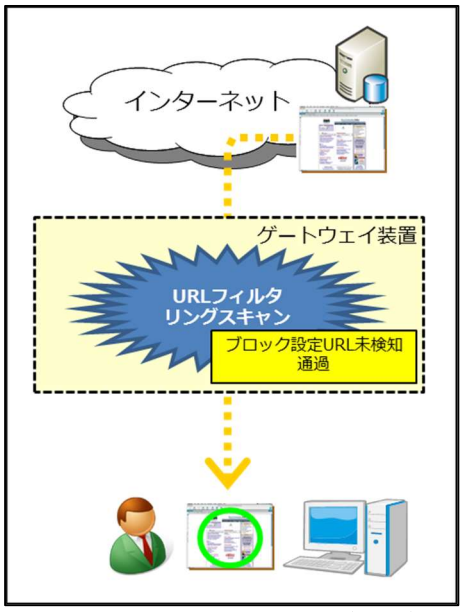


図：4-4-18「OK」を選択

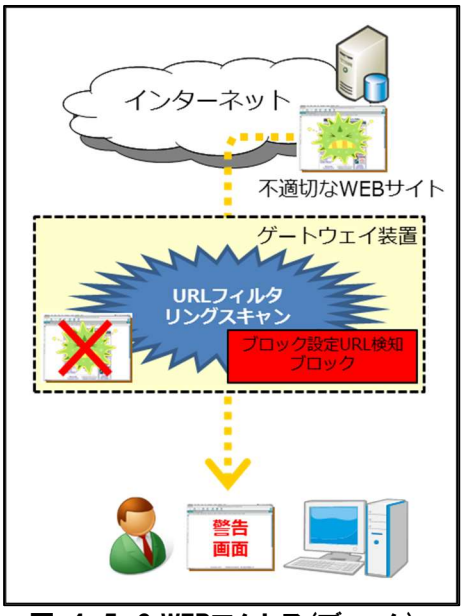
※もし、証明書インポート後に Firefox に「この接続ではプライバシーが保護されません」という表示が出てくる場合は、一度ブラウザを終了し、ブラウザを再度起動してインターネットへの接続をお試しください。

４－５ URLフィルタリング

エンドユーザがWEBサイトへのアクセスをおこなう場合、そのWEBサイトに対して、URLフィルタリングを実施します。ブロックするURLカテゴリ対象のWEBサイトへのアクセス、もしくはURLブラックリストに登録されたWEBサイトへのアクセスは、ゲートウェイ装置によってそのWEBアクセスをブロックし、エラー画面を表示します。対象外と判定された場合には、通常どおりにWEBサイトが表示されます。



図：4-5-1 WEBアクセス（通過）



図：4-5-2 WEBアクセス（ブロック）

４－５－１ 運用方法

URLフィルタリング、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

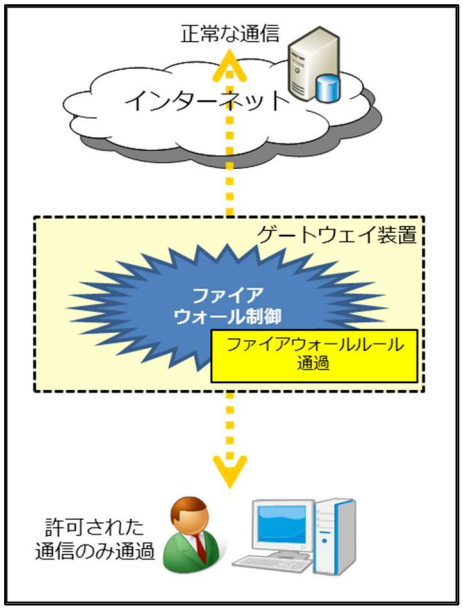
４－５－２ こんな時は・・・

【URLフィルタリングの設定を変更したい。】

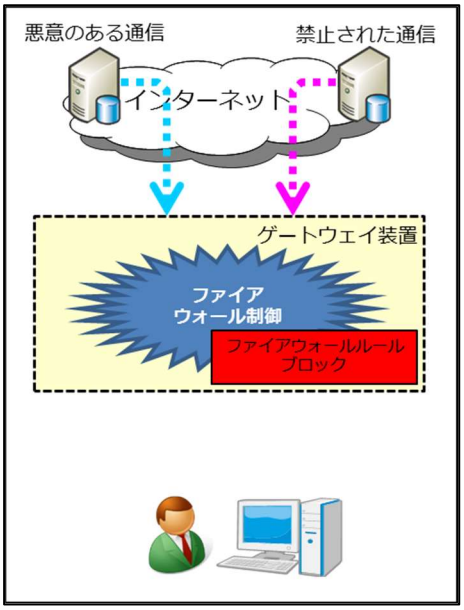
URLカテゴリフィルタリングの設定、およびURLホワイトリスト・ブラックリストの設定はお客さまにて実施可能となっています。詳細については、『４－１４ URLカテゴリフィルタ/URLホワイト・ブラックリストの設定』をご参照ください。

４－６ ファイアウォール

ゲートウェイ装置を通過するパケットを監視し、ルールに従ってパケットを制御します。



図：4-6-1 ファイアウォール（通過）



図：4-6-2 ファイアウォール（ブロック）

４－６－１ 運用方法

ファイアウォールは、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

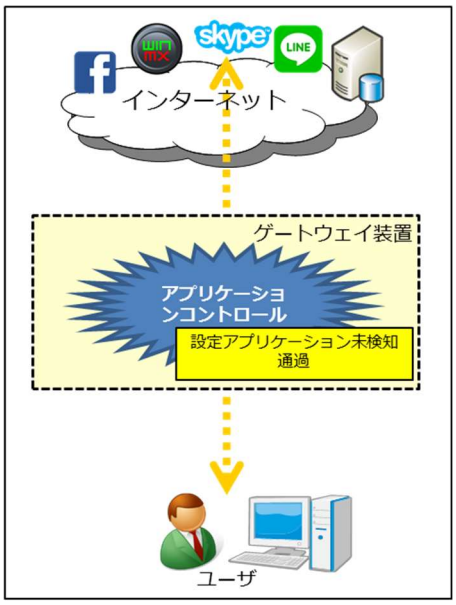
４－６－２ こんな時は・・・

【ファイアウォールのルールを変更したい。】

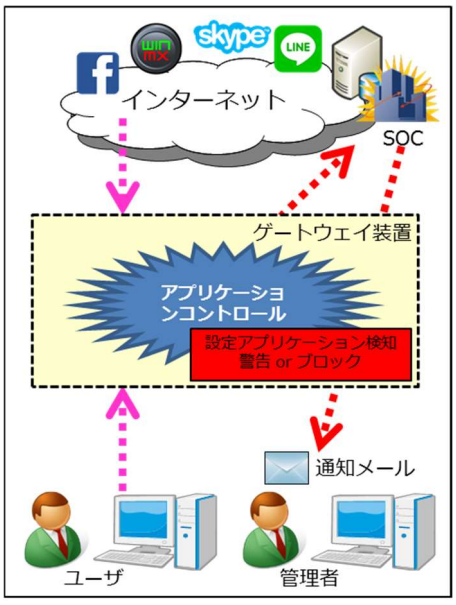
⇒ 変更サービスオーダシートのファイアウォールルールに、変更内容を記載し、SOCまで設定変更依頼をおこなってください。（『５ ユーザ・サポート・サイト』 参照）

4－7 アプリケーションコントロール

ゲートウェイ装置を通過しようとする特定アプリケーション（全29種類）の通信を監視し、お客さまが遮断を希望するアプリケーションを検知します。検知した場合は、SOCからご契約の管理者さまへその詳細を1日1回Eメールにてお知らせいたします。



図：4-7-1 アプリケーションコントロール（通過）



図：4-7-2 アプリケーションコントロール（警告/ブロック）

4－7－1 運用方法

アプリケーションコントロールは、ゲートウェイ装置にて自動でおこないます。お客さまが遮断を希望されたアプリケーションによる通信を検知した場合、SOCが検知内容を確認し、お客さまへ添付ファイル付Eメールにてご連絡いたします。報告された内容をもとに、お客さまにて対処を決定してください。

※同一送信元アドレス・送信先アドレス・検知アプリケーションの組み合わせを元に、1日5回以上の検知があった場合に添付ファイル付Eメールが送信されます。5回未満の検知の場合は送信されません。

アプリケーション検知メール内容	
To	お客さまのメールアドレス
Cc	soc-all@nttpc.co.jp
送信元	gss_imp2p@nttpc.co.jp
件名	【ゲートウェイ・セキュリティ運用監視サービス】アプリケーション検知のご報告（年月日　SB　番号　サービスID）
添付	Imp2p_SBxxxxxx_gssxxx_2014xxxx.pdf
本文	●●●　ご担当者　様 NTTPC コミュニケーションズ セキュリティ・オペレーション・センタです。 平素は格別のご高配を賜り、厚く御礼申し上げます。

お客様にて導入されている UTM 装置において、利用を制限されている
アプリケーションの通信パターンを検知いたしました。

検知日：●月●日（●）
サービス ID：gssXXX-XXXXX

検知内容の詳細については添付のレポートをご確認ください。

【補足事項】
・本機能では、ファイル交換ソフトやメッセンジャーソフトなど、
特定のアプリケーションの利用制限を目的としており、検知された
通信自体には危険性はありません。

・レポートに記載されているアプリケーションを利用していない場合は、
似たパターンの別の通信を検知している可能性があります。

・本機能の詳細については、下記 FAQ をご参照ください。
http://faq.nttpc.co.jp/faq/show/5890?site_domain=securityboss

以上、ご不明な点等ございましたら下記窓口までお問い合わせください。
どうぞよろしくお願いいたします。

■■ Security BOSS 窓口 ■■

株式会社 NTTPC コミュニケーションズ
セキュリティ・オペレーション・センタ
TEL 0120-708-602(フリーダイヤル)
E-mail: soc-all@nttpc.co.jp
FAQ　: http://www.nttpc.co.jp/faq/solution/securityboss/index.html
---

図:4-7-3 アプリケーション検知メール

アプリケーション　検知一覧(20140526)

○検知内容

送信元アドレス	検出回数（回）	検知アプリケーション	送信先アドレス	アクション（通過/遮断）
119.18.174.18	100	Winny	192.168.10.111	遮断
192.168.10.111	600	Winny	106.172.121.193	遮断
	500	Winny	59.141.169.19	遮断
	400	Winny	58.85.254.94	遮断
	300	Winny	58.3.122.110	遮断
	200	Winny	49.156.228.78	遮断
	10	Winny	121.108.79.188	遮断
	6	Winny	125.195.20.137	遮断
	5	Winny	122.209.95.243	遮断
	5	Winny	122.50.44.208	遮断

図:4-7-4 添付ファイル

【添付ファイル内容】
・送信元アドレス
アプリケーションのパケット送信元端末のIPアドレスを記載します。双方向で通信をおこなうため、通信相手も検出する可能性があります。

・検出回数
ゲートウェイ装置がアプリケーションの特徴のあるパケットを検出した回数を記載します。通信がおこなわれた場合はデータ量に比例し複数回検出されます。少数の場合は誤検知の可能性があります。

・検知アプリケーション
検知したアプリケーション名を記載します。検知可能なアプリケーションの送出するパケットの特徴と似たパケットを送出する別アプリケーションが誤検知される可能性があります。

・送信先アドレス
アプリケーションのパケット送信先のIPアドレスを記載します。双方向で通信をおこなうため、通信相手も検出する可能性があります。

・アクション（通過/遮断）
検出したアプリケーションから送信されたパケットに対するアクションを記載します。

（注）レポートにおいて通過は記載されません。全て遮断となります。

以下に対処例を記載します。

① 送信元アドレスから使用している端末を特定し、使用を中止する。
② 検知したアプリケーションの使用禁止を告知する。

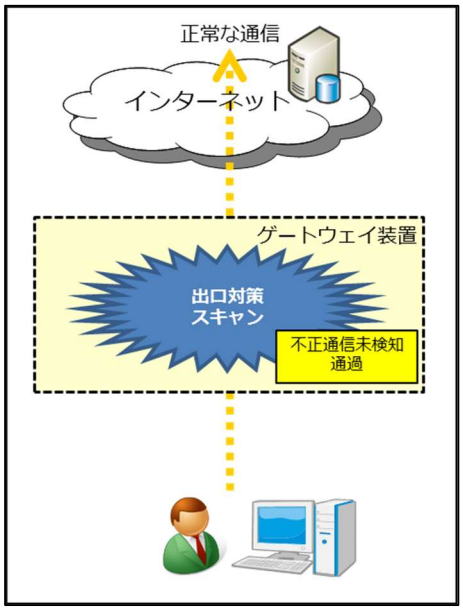
４－７－２ こんな時は・・・

【特定のアプリケーションの使用を許可したい。】

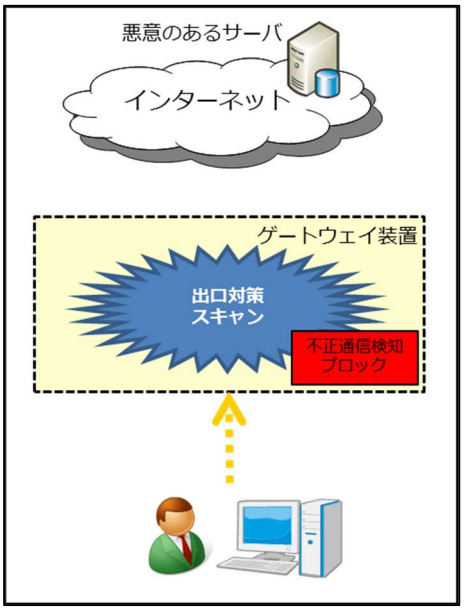
アプリケーション毎に通過/遮断の設定を、お客さまにて変更が可能です。詳細については、『４－１５ アプリケーションコントロールの設定』をご参照ください。

４－８ 出口対策

お客さまの使用されている端末がマルウェアに感染してしまった結果、端末から外部に対してお客さまの意図しない不正な通信をおこなった際に、ゲートウェイ装置を通過しようとするその通信を検知しブロックします。



図：4-8-1 出口対策（通過）



図：4-8-2 出口対策（ブロック）

４－８－１ 運用方法

出口対策は、ゲートウェイ装置にて自動でおこないます。

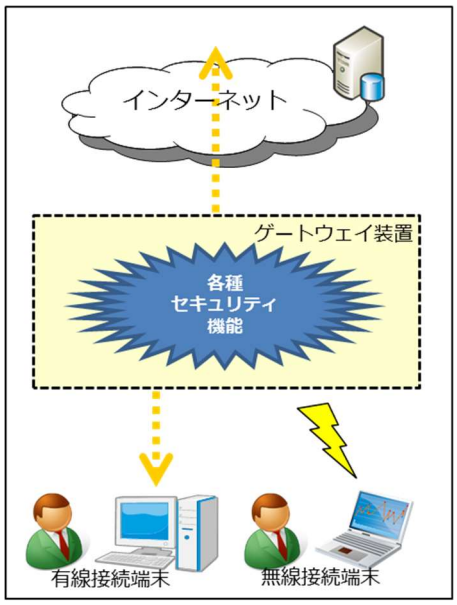
４－８－２ こんな時は・・・

【出口対策のルール（有効／無効のみ）を変更したい。】

⇒ 変更サービスオーダシートの出口対策ルールに、変更内容を記載し、SOCまで設定変更依頼をおこなってください。
（『５ ユーザ・サポート・サイト』 参照）

４－９ WiFi アクセスポイント

ゲートウェイ装置をWiFiアクセスポイントとして利用できます。WiFiで接続された端末に対しても各セキュリティ機能を提供します。（セキュリティポリシーは有線接続と無線接続で同一です。）



図：4-9-1 WiFiアクセスポイント

４－９－１ 運用方法

WiFi接続する端末の設定が必要となります。詳細は『４－９－３ 端末の設定』をご参照ください。

４－９－２ こんな時は・・・

【WiFiアクセスポイント設定を変更したい。】

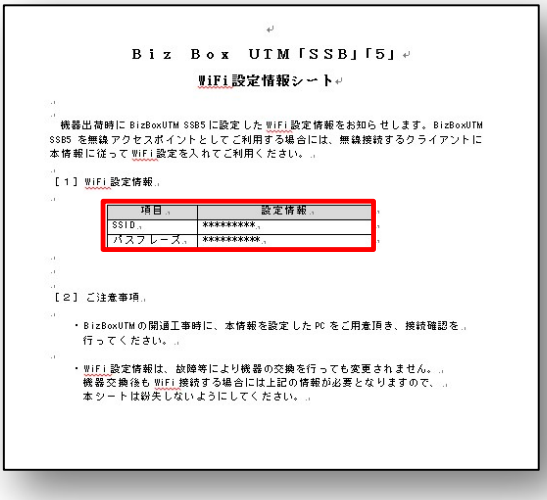
WiFi設定はお客さまにて実施可能となっています。詳細については、『４－１８ WiFiアクセスポイント設定』をご参照ください。

４－９－３ 端末の設定

ゲートウェイ装置にWiFi接続する場合、ゲートウェイ装置に設定されているWiFi設定情報と、各端末へのWiFi（無線LAN）設定が必要になります。WiFi設定情報はゲートウェイ装置に同梱されている「WiFi設定情報シート」、あるいはサービス開通時にお客さまへお知らせする「開通のご案内メール」に記載されておりますので、端末の設定の前にご準備ください。

（注）一部のお客さまにつきましては「WiFi設定情報シート」の同梱はありませんので、その場合は「開通のご案内メール」によるご確認をお願いします。

■WiFi設定情報



Ｂｉｚ Ｂｏｘ ＵＴＭ「ＳＳＢ」「５」

WiFi設定情報シート

機器出荷時に BizBoxUTM SSB5 に設定した WiFi 設定情報をお知らせします。BizBoxUTM SSB5 を無線アクセスポイントとしてご利用する場合には、無線接続するクライアントに本情報に従って WiFi 設定を入れてご利用ください。

［１］WiFi 設定情報

項目	設定情報
SSID	*********
パスフレーズ	**********

［２］ご注意事項

・BizBoxUTM の開通工事時に、本情報を設定した PC をご用意頂き、接続確認を行ってください。

・WiFi 設定情報は、故障等により機器の交換を行っても変更されません。機器交換後も WiFi 接続する場合には上記の情報が必要となりますので、本シートは紛失しないようにしてください。

図：4-9-1 WiFi設定情報シート

【WiFi 設定情報】
・SSID　　：*********
・パスフレーズ　：**********
・周波数　　：2.4GHz
※無線アクセスポイント運用が「有効」の場合にご利用頂けます。

図：4-9-2 WiFi設定情報（開通のご案内メール）

■WiFi接続端末の設定方法

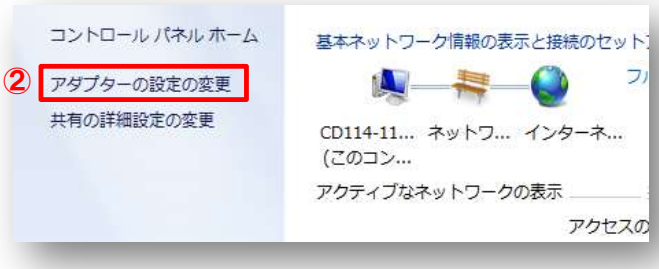
（注）端末のOS種別、OSバージョンや、端末のメーカ付属WiFi設定ツール等により、各設定画面の表示内容が異なる場合がありますので、詳細はOSや端末メーカのマニュアルを参照ください。

Windows 7の場合

①「スタート」ー「コントロールパネル」を選択して、「コントロールパネル」を開き、「ネットワークと共有センター」を押下する。

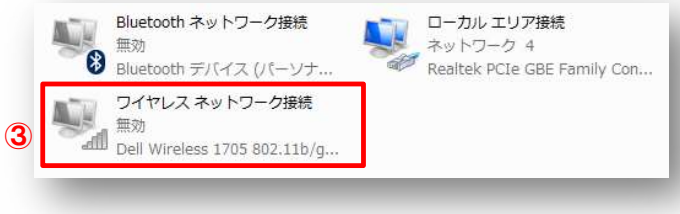
図：4-9-3 コントロールパネル画面

②「ネットワークと共有センター」を押下すると「図：4-9-4 アダプター設定画面」が表示されるので、「アダプターの設定の変更」を押下する。



図：4-9-4 アダプター設定画面

③「アダプターの設定の変更」を押下すると「図：4-9-5 ネットワーク選択画面」が表示されるので、「ワイヤレスネットワーク接続」を押下（ダブルクリック）する。



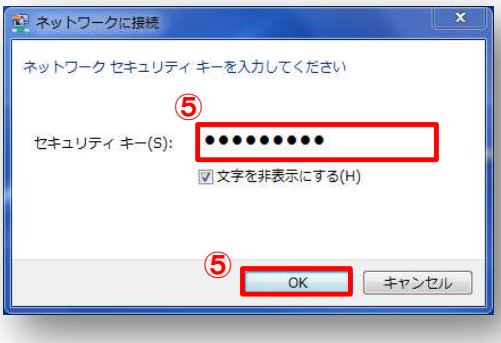
図：4-9-5 ネットワーク選択画面

④「ワイヤレスネットワーク接続」を押下（ダブルクリック）すると「図：4-9-6　アクセスポイント一覧画面」アクセスポイントの一覧が表示されるので、WiFi設定情報シートの「SSID」欄に記載されている名称と同じアクセスポイントを選択して「接続（C）」ボタンを押下する。

（注）「自動的に接続する」にチェックを入れておくと、次回の接続以降⑤の操作は不要になります。

図：4-9-6 アクセスポイント一覧画面

⑤「接続（C）」ボタンを押下すると「図：4-9-7　セキュリティキー入力画面」の入力画面が表示されるので、WiFi設定情報シートの「パスフレーズ」欄に記載されている文字列を入力して「OK」ボタンを押下する。



図：4-9-7 セキュリティキー入力画面

Windows 8.1の場合

①画面右下隅をポイントし、マウスポインターを上方向へ移動させる。チャームが表示されたら、「設定」を押下する。

図:4-9-8 トップ画面

②「設定」を押下すると「図:4-9-9 PC設定の変更画面」が表示されるので「利用可能」アイコンを押下する。

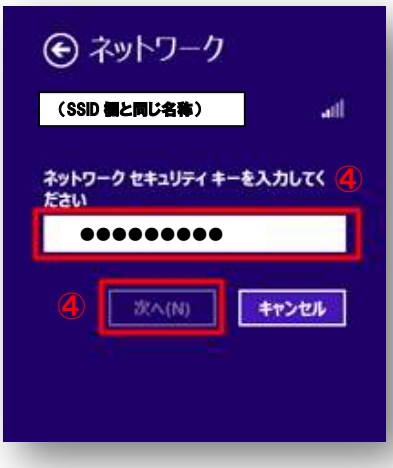
図:4-9-9 PC設定の変更画面

③「利用可能」アイコンを押下すると「図：4-9-10 アクセスポイント一覧画面」が表示されるので、WiFi設定情報シートの「SSID」欄に記載されている名称と同じアクセスポイントを選択して、「接続（C）」を押下する。

（注）「自動的に接続する」にチェックを入れておくと、次回の接続以降④の操作は不要になります。

図：4-9-10 アクセスポイント一覧画面

④「接続（C）」を押下すると「図：4-9-11ネットワークセキュリティキー入力画面」の入力画面が表示されるので、WiFi設定情報シートの「パスフレーズ」欄に記載されている文字列を入力して「次へ（N）」を押下する。



図：4-9-11 セキュリティキー入力画面

⑤「次へ(N)」を押下すると「図:4-9-12 ホームネットワーク選択画面」が表示されるので、「はい」を押下する。

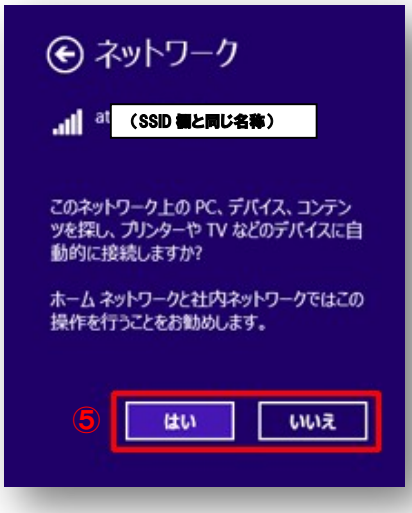


図:4-9-12 ホームネットワーク選択画面

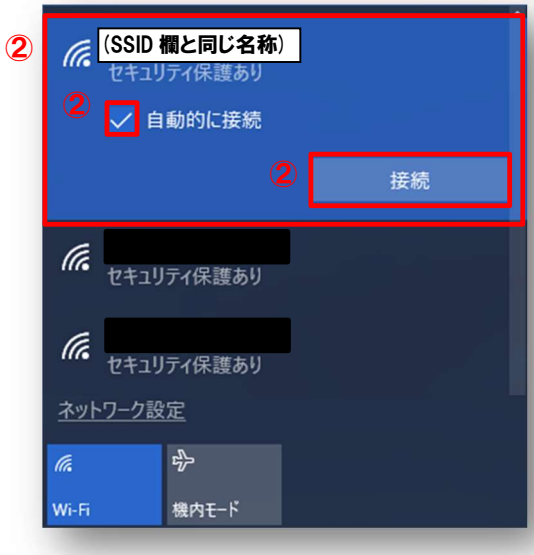
Windows 10 の場合

①デスクトップ下側に表示されているタスクバーの右側にある「WiFi」アイコンを押下する。

図:4-9-13 コントロールパネル画面

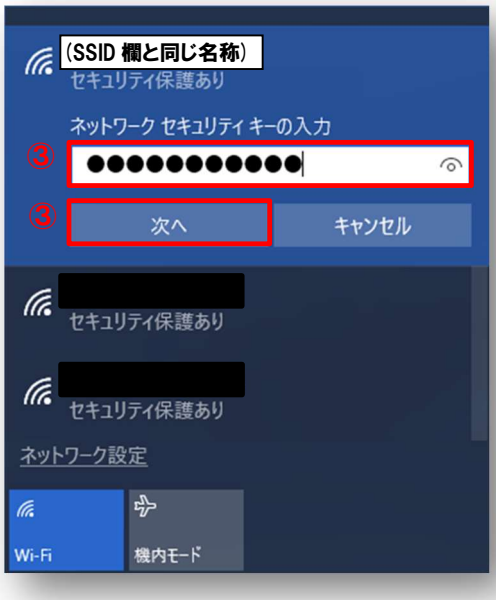
②「WiFi」アイコンを押下すると「図：4-9-14 アクセスポイント一覧画面」が表示されるので、WiFi設定情報シートの「SSID」欄に記載されている名称と同じアクセスポイントを選択して、「接続」を押下する。

（注）「自動的に接続する」にチェックを入れておくと、次回の接続以降③の操作は不要になります。



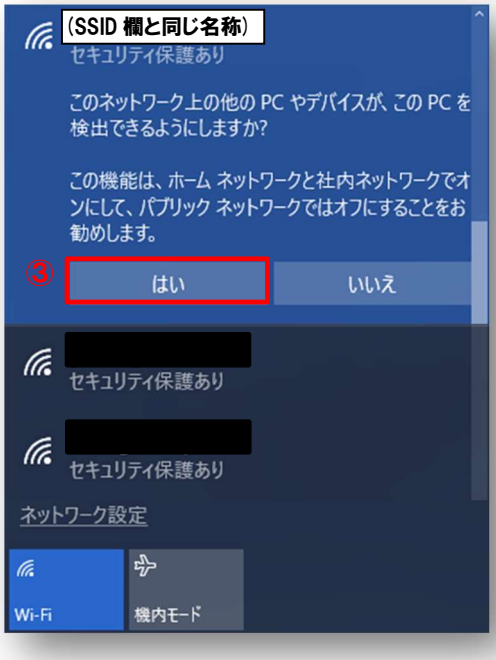
図：4-9-14 アクセスポイント一覧画面

③「接続」を押下すると「図：4-9-15 ネットワーク セキュリティキーの入力画面」が表示されるので、WiFi設定情報シートの「パスフレーズ」欄に記載されている文字列を入力して「次へ」ボタンを押下する。。



図：4-9-15 ネットワーク セキュリティキーの入力画面

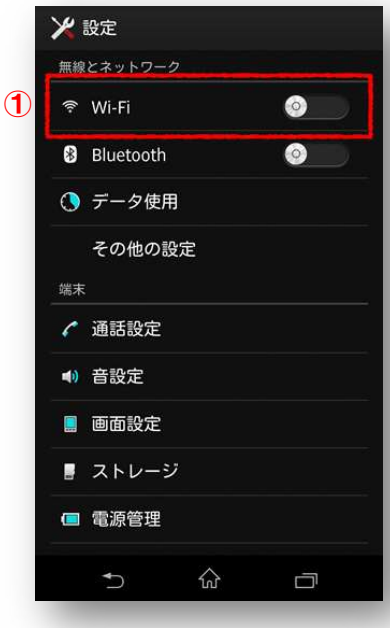
④「次へ」を押下すると「図：4-9-16 ホームネットワーク選択画面」が表示されるので、「はい」を押下する。



図：4-9-16 ホームネットワーク選択画面

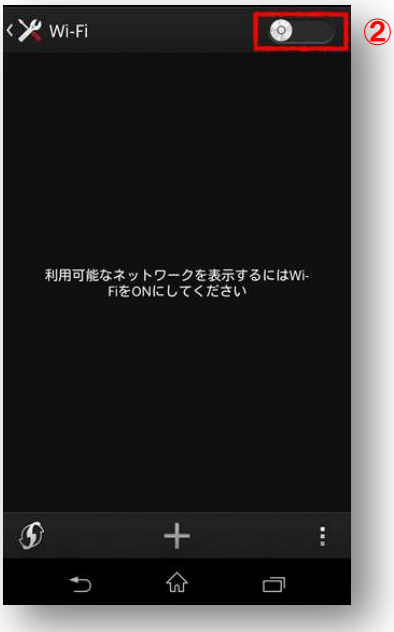
Android の場合

①「設定」の中の「無線とネットワーク」の項目にある「Wi-Fi」をタップする。



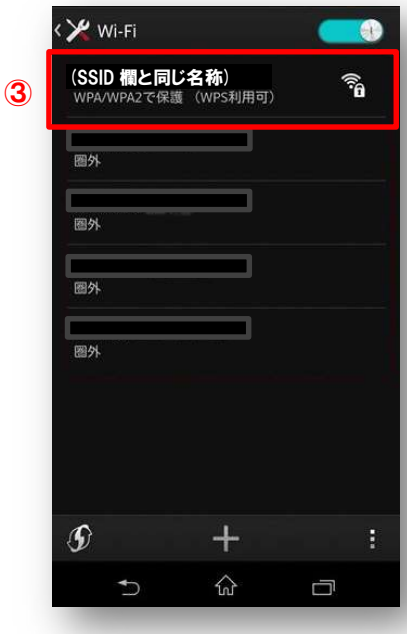
図：4-9-17 設定画面

②「Wi-Fi」をタップすると「図：4-9-18 Wi-Fi設定画面」が表示されるので、画面右上のスイッチを右にスライドしてWi-Fiを有効にする。



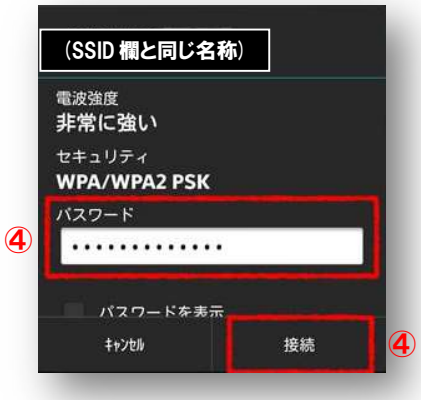
図：4-9-18 Wi-Fi設定画面

③Wi-Fiを有効にすると「図：4-9-19 アクセスポイント選択画面」の一覧が表示されるので、WiFi設定情報シートの「SSID」欄に記載されている名称と同じアクセスポイントをタップする。



図：4-9-19 アクセスポイント選択画面

④アクセスポイントをタップすると「図：4-9-20 パスワード入力画面」が表示されるので、WiFi設定情報シートの「パスフレーズ」欄に記載されている文字列を入力して接続をタップする。



図：4-9-20 パスワード入力画面

iPhoneの場合

①ホーム画面上の「設定」をタップすると「設定画面」が表示されるので、「Wi-Fi」をタップする。

図：4-9-21 設定画面

②「Wi-Fi」をタップすると「図：4-9-22 Wi-Fiネットワーク画面」が表示されるので、画面右上の「Wi-Fi」スイッチを右にスライドしてWi-Fiを有効にする。アクセスポイントの一覧が表示されるので、WiFi設定情報シートの「SSID」欄に記載されている名称と同じアクセスポイントをタップする。

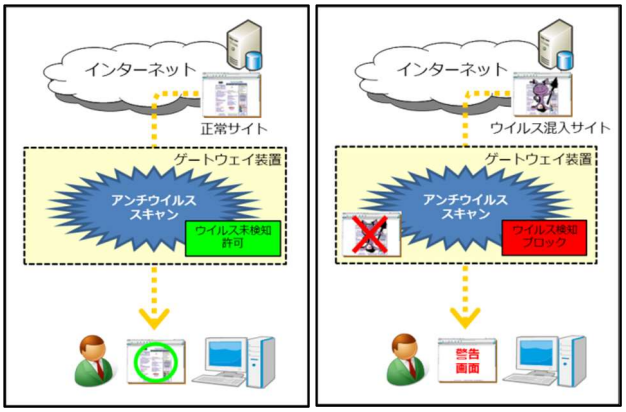
図：4-9-22 Wi-Fiネットワーク画面

③アクセスポイントをタップすると「図：4-19-23 パスワード入力画面」が表示されるので、WiFi設定情報シートの「パスフレーズ」欄に記載されている文字列を入力して「接続」をタップする。

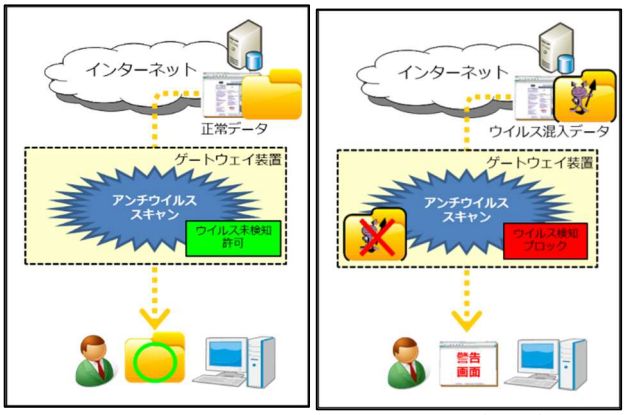
図：4-19-23 パスワード入力画面

4－10　IPv6 セキュリティ

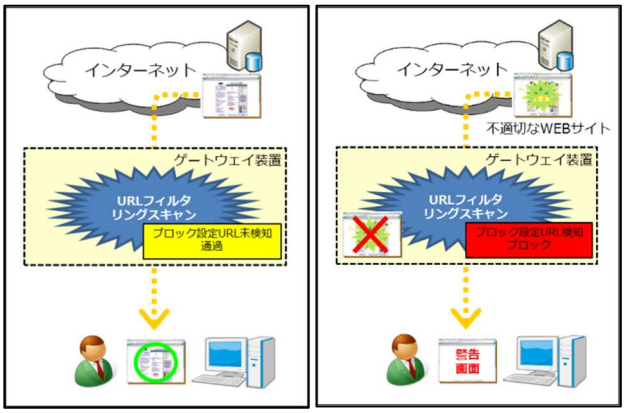
本サービスで提供している『4－4　WEB アンチウイルス』、『4－5　URLフィルタリング』、『4－6　ファイアウォール』について、これまでの対象であった IPv4 アドレスに対する機能を IPv6 アドレスについても提供します。



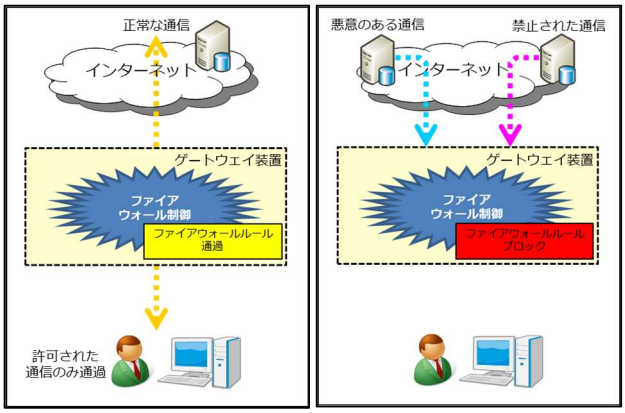
図：4-10-1 WEB アンチウイルス（IPv6）



図：4-10-2　ダウンロードマネージャ（IPv6）



図：4-10-3 URL フィルタリング（IPv6）



図：4-10-4　ファイアウォール（IPv6）

4－10－1　運用方法

IPv6セキュリティは、ゲートウェイ装置にて自動でおこないます。特別な管理は必要ありません。

4－10－2　ご注意事項

【ISP と IPv6 インターネットサービスを契約している場合のみ「有効」としてください。】

IPv6 セキュリティ機能を利用する場合は、必ず ISP と IPv6 インターネットサービスを契約していることを確認したうえで「有効」としてください。（NTT フレッツ IPv6 サービスは閉域網で提供されるサービスとなりインターネットサービスとは異なります。）

【ご使用の端末に IPv6 アドレスが自動付与されているかを確認してください。】

お客さま利用端末が IPv6 アドレスを取得していない場合、または手動（固定）で IPv6 アドレスを取得している場合は、IPv6 セキュリティ機能は必ず「無効」としてください。上記環境では IPv6 セキュリティ機能を「有効」にした場合、Biz Box UTM が IPv6 アドレスを自動取得できないため、IPv6 通信が正常に行われませんのでご注意ください。

４－１０－３ こんな時は・・・

【IPv6セキュリティ設定を変更したい。】

変更サービスオーダシートの各セキュリティ機能欄に変更内容を記載し、SOC まで設定変更依頼をおこなってください。（『５ ユーザ・サポート・サイト』 参照）

４－１１　カスタマコントロール・ログイン方法

本サービスでは次項の『４－１２　メール送信者ホワイトリスト設定』、『４－１３　POP3サーバ設定』、『４－１４　URLカテゴリフィルタ/URLホワイト・ブラックリスト設定』、『４－１５　WEBスキャンスキップ設定』、『４－１６　アプリケーションコントロール設定』、『４－１７　WiFiアクセスポイント設定』により、ゲートウェイ装置の一部設定をお客さまにて実施することが可能となっております。本項では、設定変更のためのカスタマコントロールへのログイン方法を説明します。

ログイン操作手順は以下のとおりです。

■カスタマコントロール・ログイン方法
①お客さまの使用されているWEBブラウザのアドレスバーに以下のURLを入力しアクセスする。
【URL】https://（ゲートウェイ装置に設定したIPアドレス）:4444　（例：https://172.30.0.2:4444）

初回ログイン時に以下の画面が表示されるのでご使用のWEBブラウザにより、以下の操作を実行する。

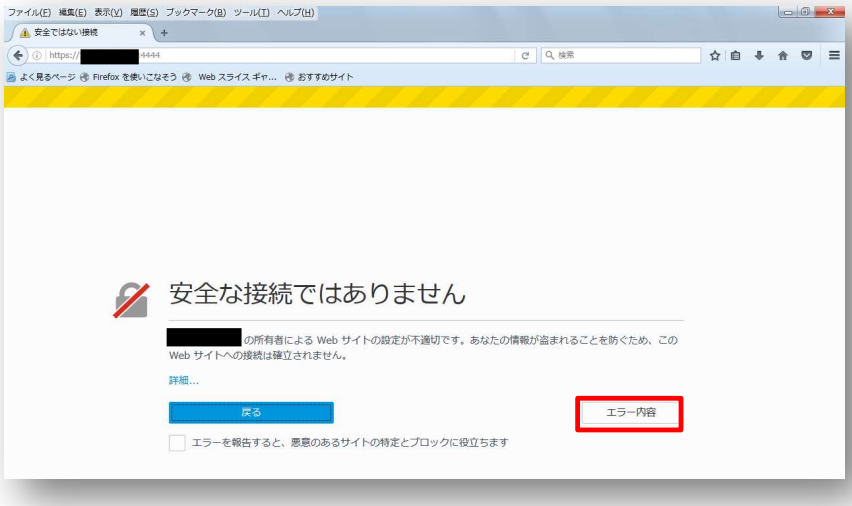
【Internet Explorer 11の場合】
「図：4-11-1　証明書に関するセキュリティの警告画面（Internet Explorer 11）」が表示されるので、「このサイトの閲覧を続行する（推奨されません）。」を押下する。

図：4-11-1　証明書に関するセキュリティの警告画面（Internet Explorer 11）

（注）ブラウザのバージョンにより画面表示が異なることがあります。

（注）ログイン画面が表示されるまでに数十秒から1分程度の時間がかかる場合があります。

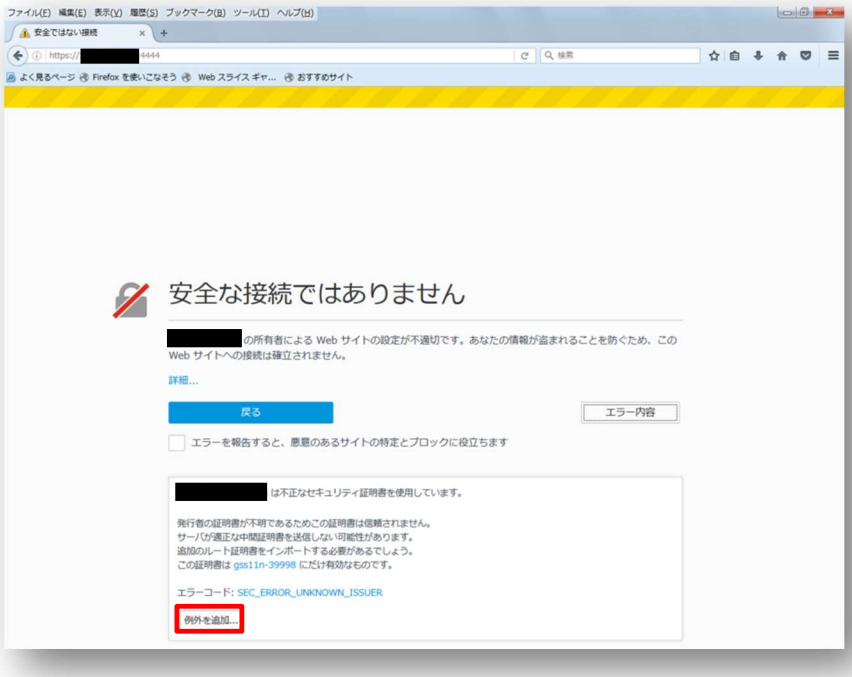
【Firefox 49の場合】
「図：4-11-2　証明書に関するセキュリティの警告画面（Firefox 49）①」が表示されるので、「エラー内容」ボタンを押下する。



図：4-11-2　証明書に関するセキュリティの警告画面（Firefox 49）①

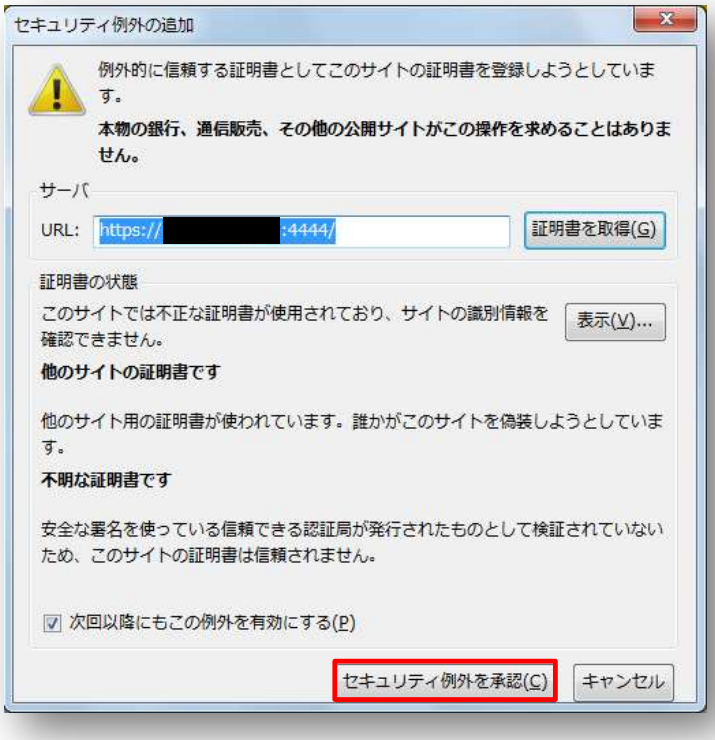
（注）ブラウザのバージョンにより画面表示が異なることがあります。

「エラー内容」ボタンを押下すると「図：4-11-3　証明書に関するセキュリティの警告画面（Firefox 49）②」となるので、画面下部に表示された「例外を追加」ボタンを押下する。



図：4-11-3　証明書に関するセキュリティの警告画面（Firefox 49）②

「例外を追加」アイコンを押下すると新たに「図：4-11-4 セキュリティ例外の追加画面 (Firefox 49)」が表示されるので、「セキュリティ例外を承認(C)」ボタンを押下する。



図：4-11-4 セキュリティ例外の追加画面 (Firefox 49)

(注)ログイン画面が表示されるまでに数十秒から1分程度の時間がかかる場合があります。

【Microsoft Edge 38の場合】
「図:4-11-5 証明書に関するセキュリティの警告画面(Microsoft Edge 38)」が表示されるので、「このWebページの閲覧を続ける(推奨されません)」を押下する。

図:4-11-5 証明書に関するセキュリティの警告画面(Microsoft Edge 38)

(注)ブラウザのバージョンにより画面表示が異なることがあります。

(注)ログイン画面が表示されるまでに数十秒から1分程度の時間がかかる場合があります。

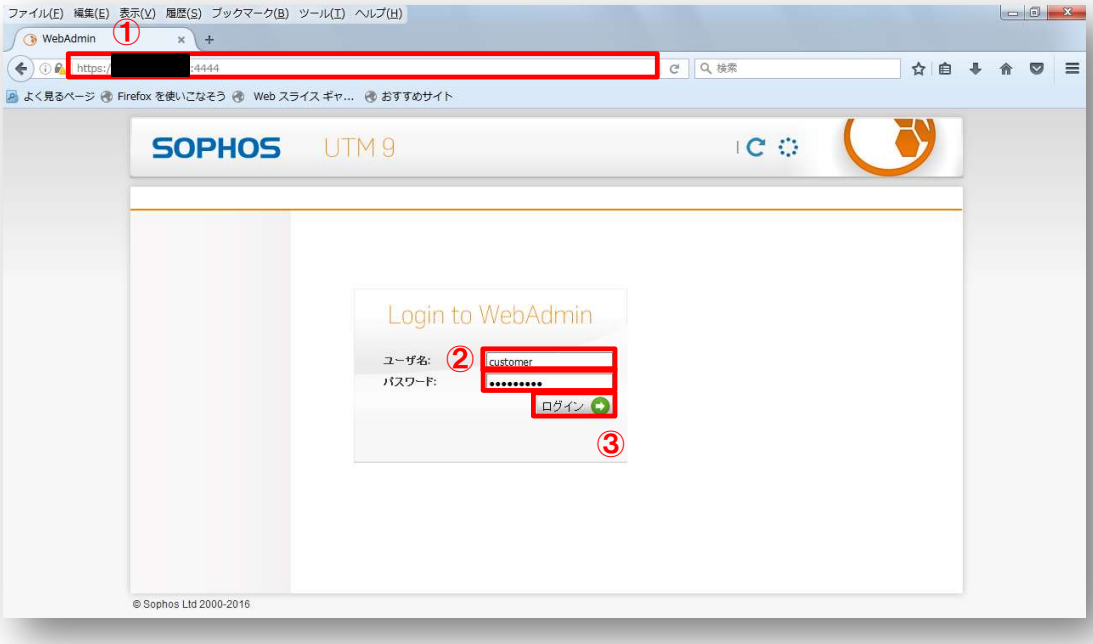
②①の操作が完了すると「図：4-11-6 カスタマコントロール・ログイン画面」が表示されるので以下の情報を入力する。

【ユーザ名】customer
【パスワード】bizboxssb

③「ログイン」アイコンを押下してログインする。

※ユーザ名もしくはパスワードを3回連続誤って入力すると、その後正常な情報を入力しても10分間ログインができなくなりますのでご注意ください。

※上記①②の情報は、本サービスのお申込み後お客さま宛に送付される「登録内容通知書」下部に同じく①カスタマコントロールURL②ログインアカウント：アカウント/パスワードとして記載されています。



図：4-11-6 カスタマコントロール・ログイン画面

4－12 メール送信者ホワイトリスト設定

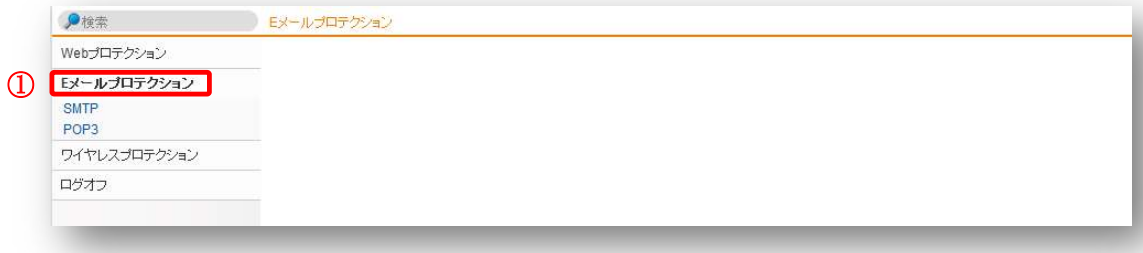
(注) 本項の対象となるゲートウェイ装置はBiz Box UTM「SSB」「Standard／Professional」、「SG125w rev3」です。Biz Box UTM「SSB」「5」、「SG105w rev3」は対象外です。

本サービスで提供する「メールアンチスパム・アンチウィルス」により、正常なEメールがスパムとして誤判定されてしまうことがあります。その場合は、送信者をホワイトリストに登録することで問題を回避することが可能です。設定はお客さまにて実施することが可能です。

設定する操作手順は以下のとおりです。

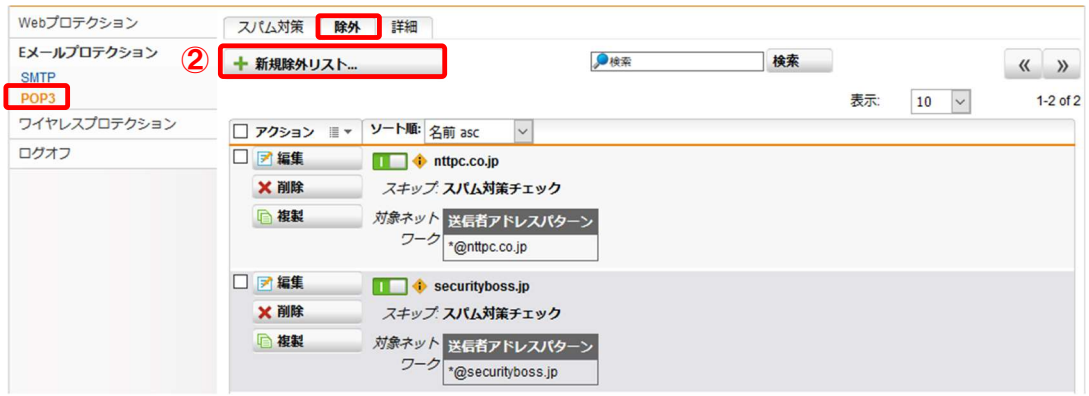
■カスタマコントロール・ログイン方法
『4－11 カスタマコントロール・ログイン方法』をご参照ください。

■メール送信者ホワイトリスト（アンチスパム除外リスト）設定方法
①ログインが成功すると以下の画面「図：4-12-1 カスタマコントロール・ログイン直後画面1」が表示されるので画面左側の「Eメールプロテクション」を押下する。



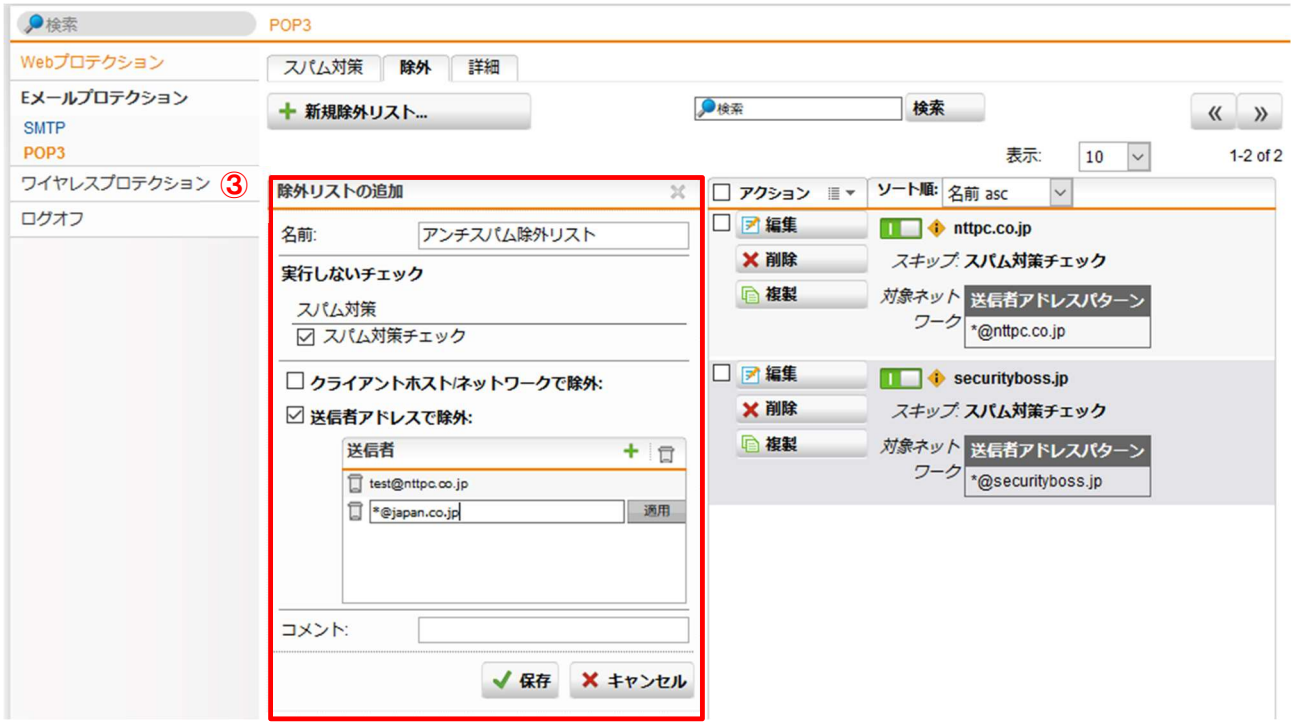
図：4-12-1 カスタマコントロール・ログイン直後画面

②画面左側の「POP3」を押下すると、以下の画面「図：4-12-2 メール送信者ホワイトリスト（アンチスパム除外リスト）設定画面」が表示されるので、画面左上の「新規除外リスト」ボタンを押下する。



図：4-12-2 メール送信者ホワイトリスト（アンチスパム除外リスト）設定画面

③「新規除外リスト」ボタンを押下すると画面左に「図：4-12-3 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面」が表示される。



図：4-12-3 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面

④「図：4-12-4 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面（拡大）」の「名前」欄に適当な名前を入力する。

⑤「アンチスパム（スパム対策チェック）」と「送信者アドレスで除外」のチェックボックスにチェックを入れ、「送信者」欄の「＋」アイコンを押下した後に表示される入力欄にメールアドレスを入力した後、「適用」ボタンを押下する。

⑥任意で「コメント」欄にコメントを入力した後、最後に「保存」ボタンを押下する。

図：4-12-4 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面（拡大）

（注）「図：4-12-4 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面（拡大）」では、1つの「名前」に対して複数の送信者メールアドレスが入力可能です。

（注）「図：4-12-4 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面（拡大）」では、「@」前のアカウント名に「＊」（ワイルドカード）を使用することで同一ドメイン全てのメールアドレスを「メール送信者ホワイトリスト（アンチスパム除外リスト）」として設定することが可能です。（例：＊@nttpc.co.jp）

（注）「図：4-12-4 メール送信者ホワイトリスト（アンチスパム除外リスト）の作成画面（拡大）」には、アンチウイルスを除外するチェックボックスが表示されている場合（ゲートウェイ装置の種類またはファームウェアのバージョンにより異なります。）がありますが、本設定は「有効」としないでください。「有効」とした場合、万が一当該メール送信者からウイルスの含まれたメールを送信された場合、ゲートウェイ装置で検知することができなくなります。

⑦「保存」ボタンを押下すると元の画面「図：4-12-5 メール送信者ホワイトリスト（アンチスパム除外リスト）設定画面②」に戻るので、④で入力した「名前」が表示されていることを確認する。

図：4-12-5 メール送信者ホワイトリスト（アンチスパム除外リスト）設定画面②

（注）設定を一時的に解除したい場合は、設定した「名前」の左側にある緑色のボタンを押下し設定を「無効」とすることが可能です。再度「有効」としたい場合は同じボタン（灰色）を再度押下してください。設定を削除したい場合は、「削除」ボタンアイコンを押下してください。

（注）サービス初期設定として「メール送信者ホワイトリスト（アンチスパム除外リスト）」に「securityboss.jp」他が表示されています。本設定はゲートウェイ装置よりまたはSOCより配信されるメールアドレスが登録されていますので絶対に削除しないでください。

（注）操作をしない時間が5分を超えた場合、自動的にログオフとなりますので、その際は再度ログインを行ってください。

4－13 POP3 サーバ設定

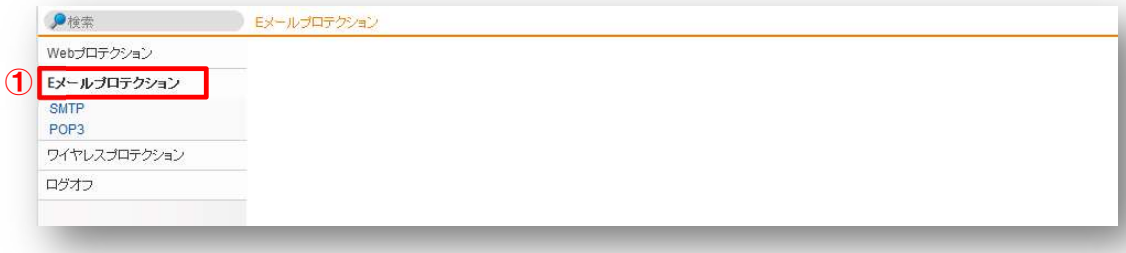
(注) 本項の対象となるゲートウェイ装置はBiz Box UTM「SSB」「Standard／Professional」、「SG125w rev3」です。Biz Box UTM「SSB」「5」、「SG105w rev3」は対象外です。

本サービスで提供する「メールアンチスパム・アンチウイルス」により、ゲートウェイ装置にてスパムメールおよびウイルスメールを隔離する対象となるお客さまの使用するPOP3サーバ（メール受信サーバ）が追加または変更となった場合、お客さまにて設定することが可能です。

設定する操作手順は以下のとおりです。

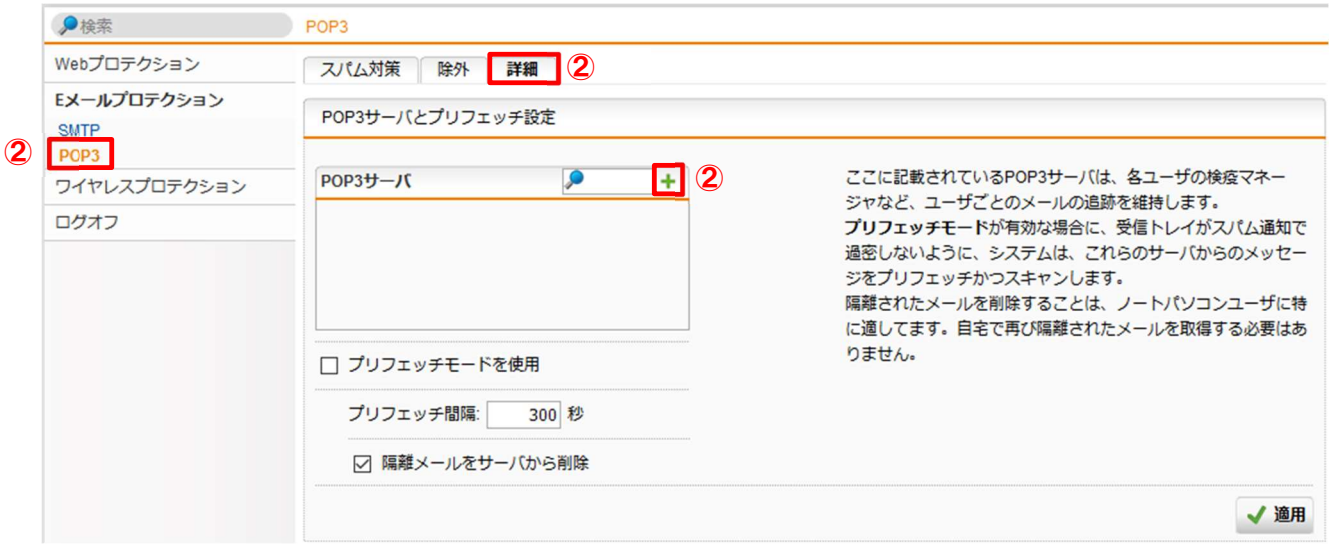
■カスタマコントロール・ログイン方法
『4－11 カスタマコントロール・ログイン方法』をご参照ください。

■POP3サーバ設定方法
①ログインが成功すると以下の画面「図：4-13-1 カスタマコントロール・ログイン直後画面」が表示されるので画面左側の「Eメールプロテクション」を押下する。



図：4-13-1 カスタマコントロール・ログイン直後画面

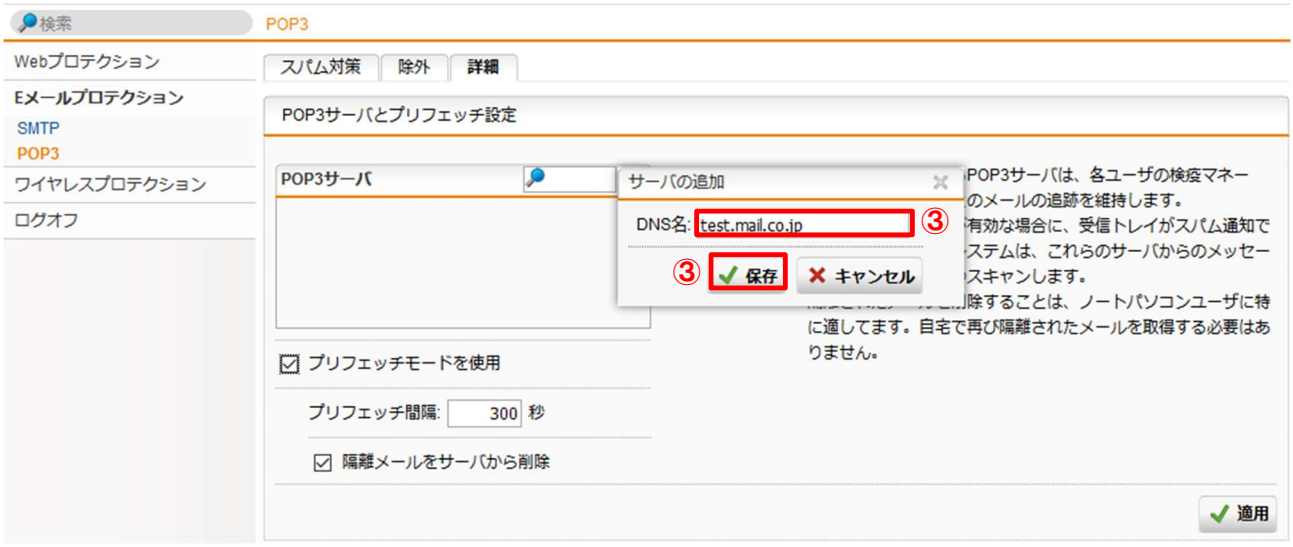
②画面左側の「POP3」を押下後、画面上の「詳細」タブを押下すると、以下の画面「図：4-13-2 POP3サーバ設定画面①」が表示されるので、「POP3サーバ」欄の「＋」アイコンを押下する。



図：4-13-2 POP3サーバ設定画面①

(注)「図：4-13-2 POP3サーバ設定画面①」にて、設定前に「POP3サーバ」欄が空欄（既存のPOP3サーバ登録なし）の場合、現在の設定は「警告」設定（スパムメール・ウイルスメールをゲートウェイ装置に隔離しない設定）となっています。その場合追加登録設定はできませんので、『５－４ サービス内容の変更』に従い「警告」設定へ変更後③以降の操作を行ってください。

③「＋」アイコンを押下すると「図：4-13-3 サーバの追加設定画面」がポップアップ表示されるので、「DNS名」に追加するPOP3サーバ（メール受信サーバ）を設定し「保存」ボタンを押下する。



図：4-13-3 サーバの追加設定画面

④「保存」ボタンを押下すると元の画面「図：4-13-4 POP3サーバ設定画面②」に戻るので、③で入力したPOP3サーバ（メール受信サーバ）が表示されていることを確認し、「適用」ボタンを押下する。

図：4-13-4 POP3サーバ設定画面②

（注）既存のPOP3サーバ（メール受信サーバ）を削除・変更する場合、削除・変更する以前に隔離されたメールは削除・変更後はゲートウェイ装置よりリリースすることが不可となります。そのため、ゲートウェイ装置に隔離された必要なメールは必ず事前に隔離レポート（「４－３ 隔離レポート（Quarantine Report）」参照）よりリリースを行った後に削除・変更を行ってください。

（注）既存のPOP3サーバ（メール受信サーバ）を削除する場合は、「POP3サーバ」欄の「×」アイコンを押下して削除、変更する場合は「編集」アイコンを押下して③を実施し、最後に④に従い設定確認後に「適用」ボタンを押下してください。

（注）追加・変更を行うPOP3サーバ（メール受信サーバ）が、アルファベット投入ミス等により誤った設定となってしまった場合、追加・変更後にゲートウェイ装置にスパムメール・ウイルスメールと判定され隔離されたメールはリリース不可となりますので、十分注意の上設定を行ってください。

（注）既存のPOP3サーバ（メール受信サーバ）を全て削除し「POP3サーバ」欄を空欄とする場合は、ゲートウェイ装置の動作仕様上「隔離」設定より「警告」設定に変更する必要がありますので、『５－４ サービス内容の変更』に従い「警告」設定へ変更後に削除を行ってください。

（注）操作をしない時間が5分を超えた場合、自動的にログオフとなりますので、その際は再度ログインを行ってください。

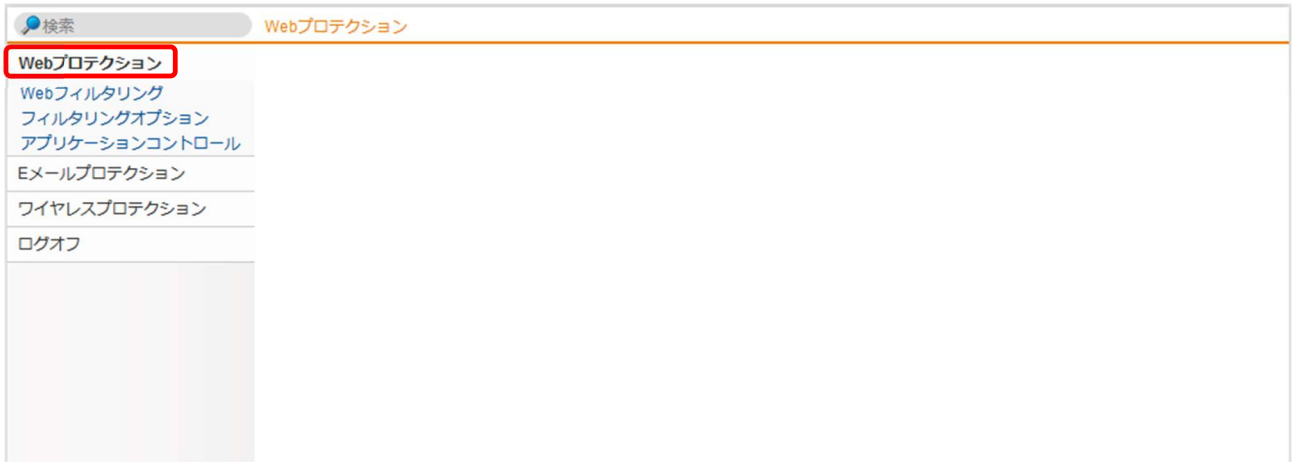
4－14　URL カテゴリフィルタ/URL ホワイト・ブラックリスト設定

本サービスで提供する「URLカテゴリフィルタリング」、または「URLホワイト・ブラックリスト」により、ゲートウェイ装置配下からのWEBアクセスを制限したい場合、または、WEBアクセスを制限されたURLカテゴリから、任意のURLのみアクセス可能としたい場合は、お客さまにて設定することが可能です。

設定する操作手順は以下のとおりです。

■カスタマコントロール・ログイン方法
『4－11　カスタマコントロール・ログイン方法』をご参照ください。

■URLカテゴリフィルタ設定方法
①ログインが成功すると以下の画面「図：4-14-1　カスタマコントロール・ログイン直後画面」が表示されるので画面左側の「Webフィルタリング」を押下する。

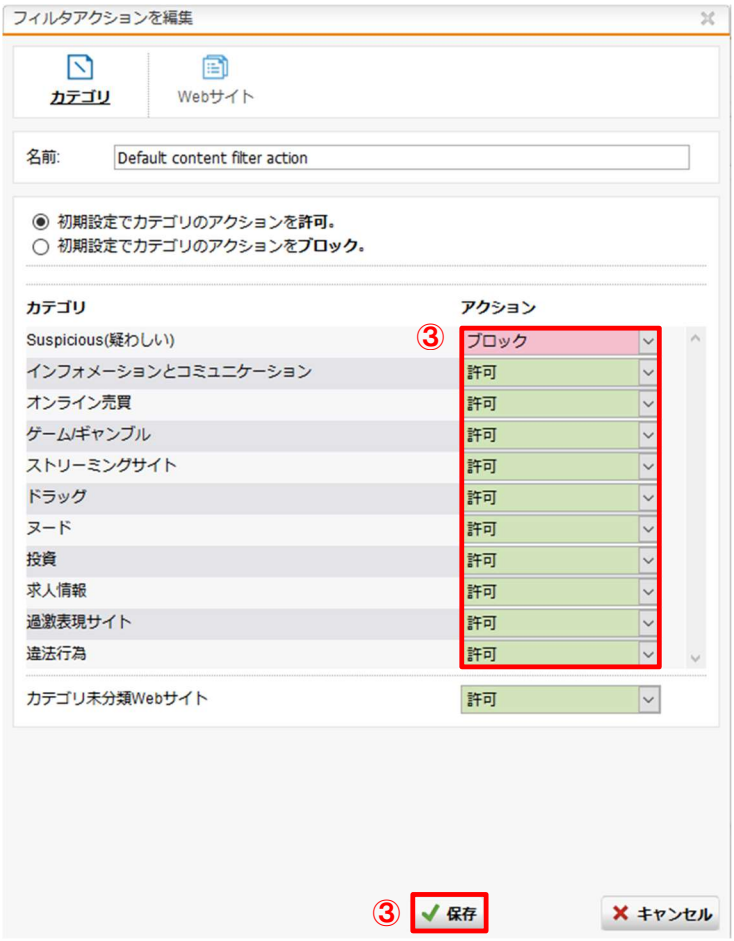


図：4-14-1　カスタマコントロール・ログイン直後画面

②画面左側の「Web フィルタリング」を押下すると、以下の画面「図：4-14-2 Web フィルタリング　ポリシー設定画面」が表示されるので、画面右側の「Default content filter action」を押下する。

図：4-14-2 Webフィルタリング　ポリシー設定画面

③「Default content filter action」を押下すると、以下の画面「図：4-14-3 フィルタアクションを編集画面」が表示されるので、「ブロック」したいカテゴリについて、画面右側のプルダウンメニューの「▼」を押下して、「ブロック」を選択、または「許可」したいカテゴリについては、同様にプルダウンメニューより「許可」を選択して、最後に下部の「保存」ボタンを押下する



図：4-14-3 フィルタアクションを編集画面

（注）プルダウンメニューからは「ブロック」または「許可」のどちらかを選択してください。「警告」と「割当て」は選択しないでください。

（注）サービス初期設定として「Suspicious（疑わしい）」がブロックに設定されています。セキュリティ上本設定は有効（ブロック）のままでご使用することをお勧めいたします。ただしスパイウェアサイトについては、本設定を無効（許可）としてもゲートウェイ装置の仕様上、ブロック対象のままとなります。

（注）操作をしない時間が5分を超えた場合、自動的にログオフとなります。その際は再度『４－１１　カスタマコントロール・ログイン方法』の②よりログインを行ってください。

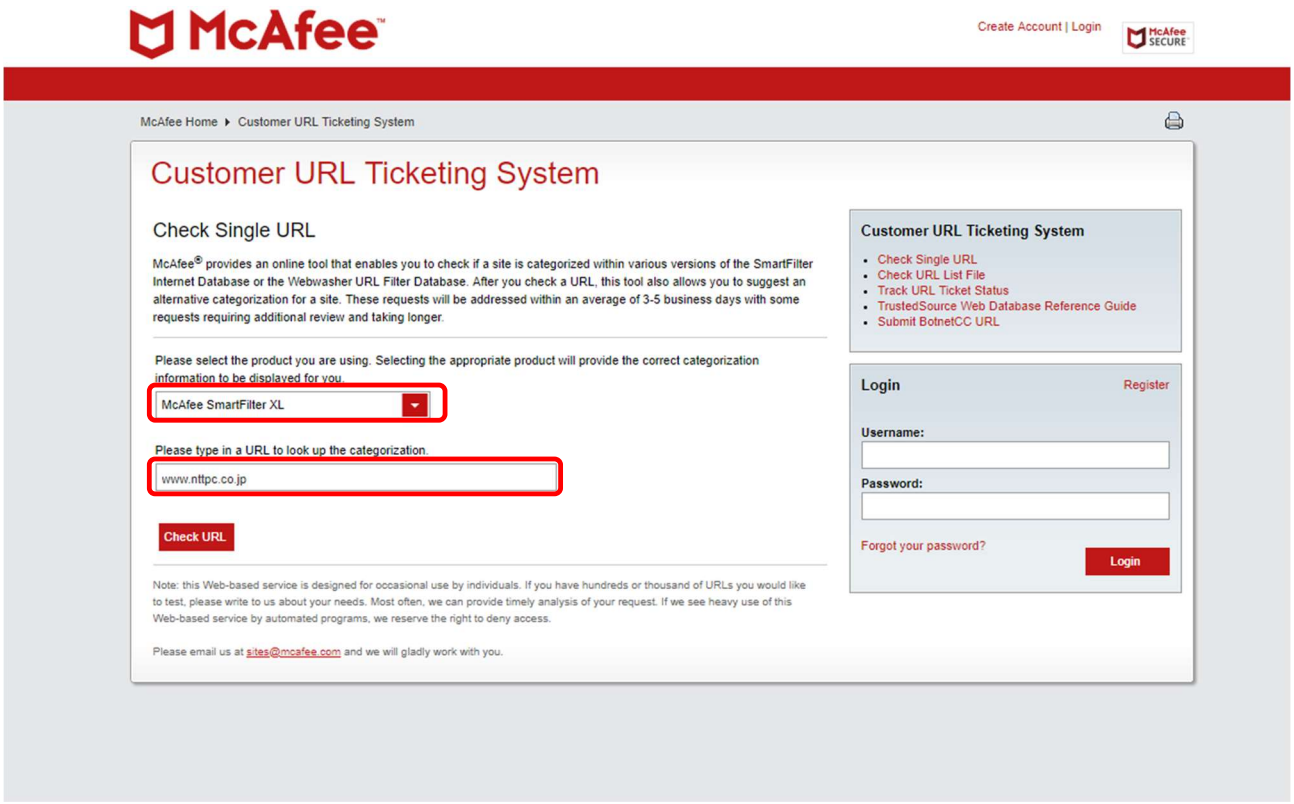
【URLカテゴリリスト】

URLカテゴリ	URLサブカテゴリ	URLサブカテゴリ（英語表記）
Suspicious（疑わしい）	悪意のあるサイト	Malicious Site
	パークドメイン	Parked Domain
	フィッシング	Phishing
	スパムURL	Spam URLs
	スパイウェア/アドウェア	Spyware/Adware
インフォメーションとコミュニケーション	チャット	Chat
	フォーラム/掲示板	Forum/Bulletin Boards
	管理されたサイト（掲示板、チャットなど）	Moderated
オンライン売買	オークション/クラシファイド広告	Auctions/Classifieds
	オンラインショッピング	Online Shopping
ゲーム/ギャンブル	ギャンブル	Gambling
	ギャンブル関連	Gambling Related
	ゲーム	Games
ストリーミングサイト	ストリーミングメディア	Streaming Media
ドラッグ	ドラッグ	Drugs
ヌード	ポルノ	Pornography
	挑発的服装	Provocative Attire
	付随的なヌード	Incidental Nudity
	ヌード	Nudity
	性的な記述・素材	Sexual Materials
	不敬、冒涜サイト	Profanity
投資	株取引	Stock Trading
求人情報	求人情報	Job Search
過激表現サイト	過激残虐な内容	Extreme
	暴力的なゲーム/漫画	Game/Cartoon Violence
	グロテスク、不快なコンテンツ	Gruesome Content
	暴力	Violence
違法行為	違法行為	Criminal Activities
	ハッキング/コンピュータ犯罪	Hacking/Computer Crime
	違法ソフト	Illegal Software
	悪意のあるダウンロード	Malicious Downloads
	怪しいプログラム	Potential Unwanted Programs

※上記のリストは、設定可能なカテゴリフィルタリングの項目とそのカテゴリに属するサブカテゴリとなります。

※個別のURLがどのカテゴリに所属するかを確認するには、以下のサイト「図：4－14-4　個別URLカテゴリ確認サイト画面」へアクセスした後、ドロップダウンメニューから「McAfee SmartFilter XL」を選択し、その下にあるBOXへURLを入力し、「Check URL」アイコンをクリックすることで結果が取得可能です。

【URL】http://www.trustedsource.org/en/feedback/url?action=checksingle

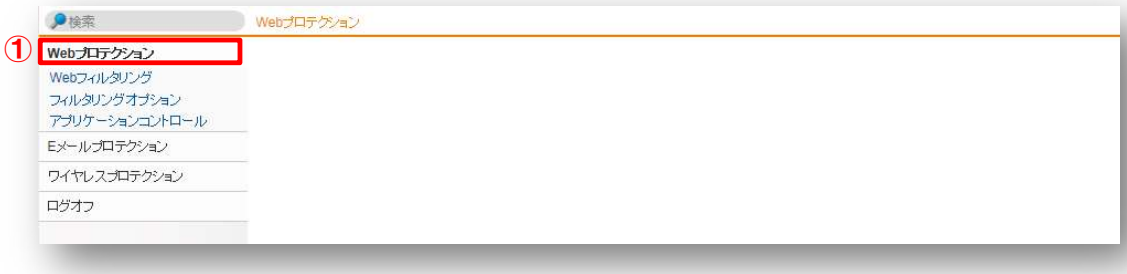


図：4-14-4　個別URLカテゴリ確認サイト画面

■URLカテゴリに含まれるサブカテゴリの変更

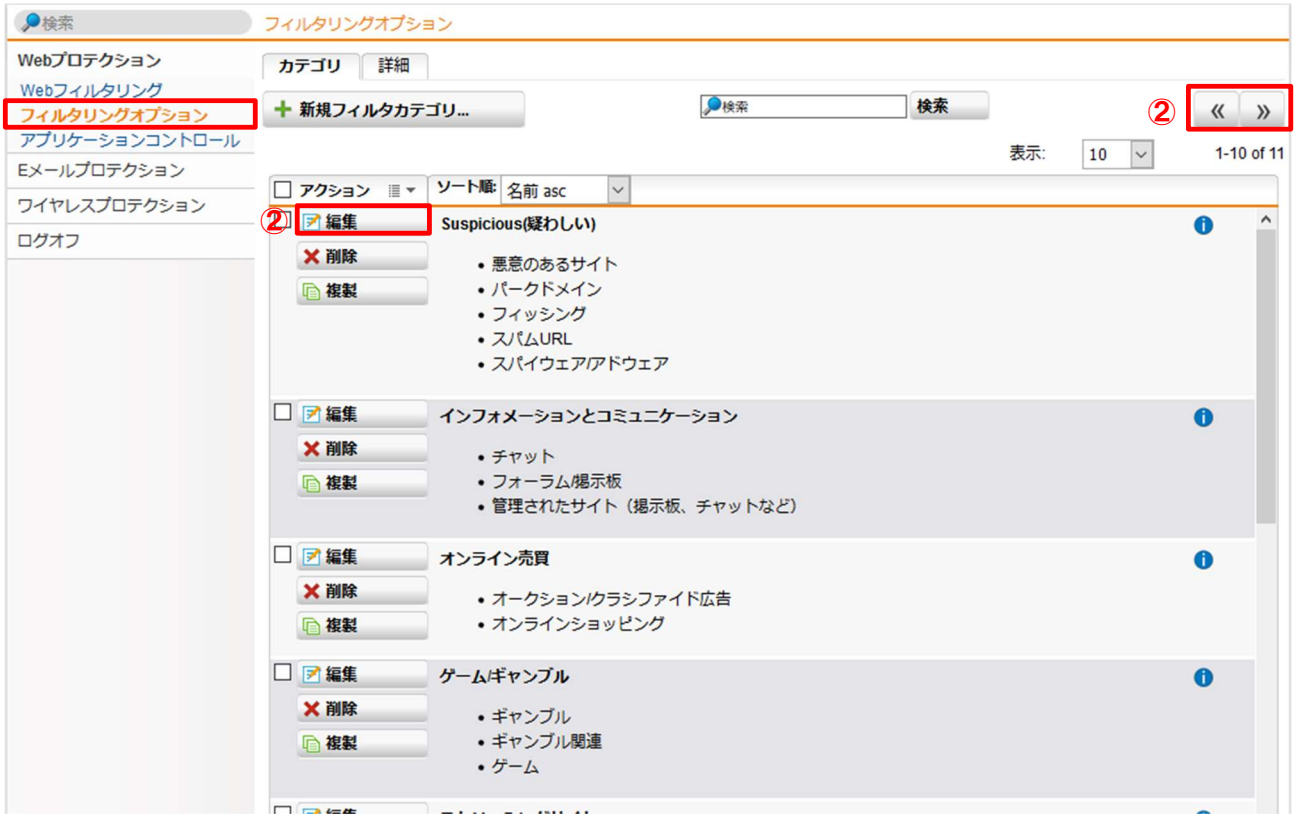
お客さまの任意にカテゴリの名前の変更、またカテゴリに含まれるサブカテゴリ（②以降参照）を変更することができます。

① ログインが成功すると以下の画面「図：4-14-5 カスタマコントロール・ログイン直後画面」にて、画面左側の「Webプロテクション」を押下する。



図：4-14-5 カスタマコントロール・ログイン直後画面

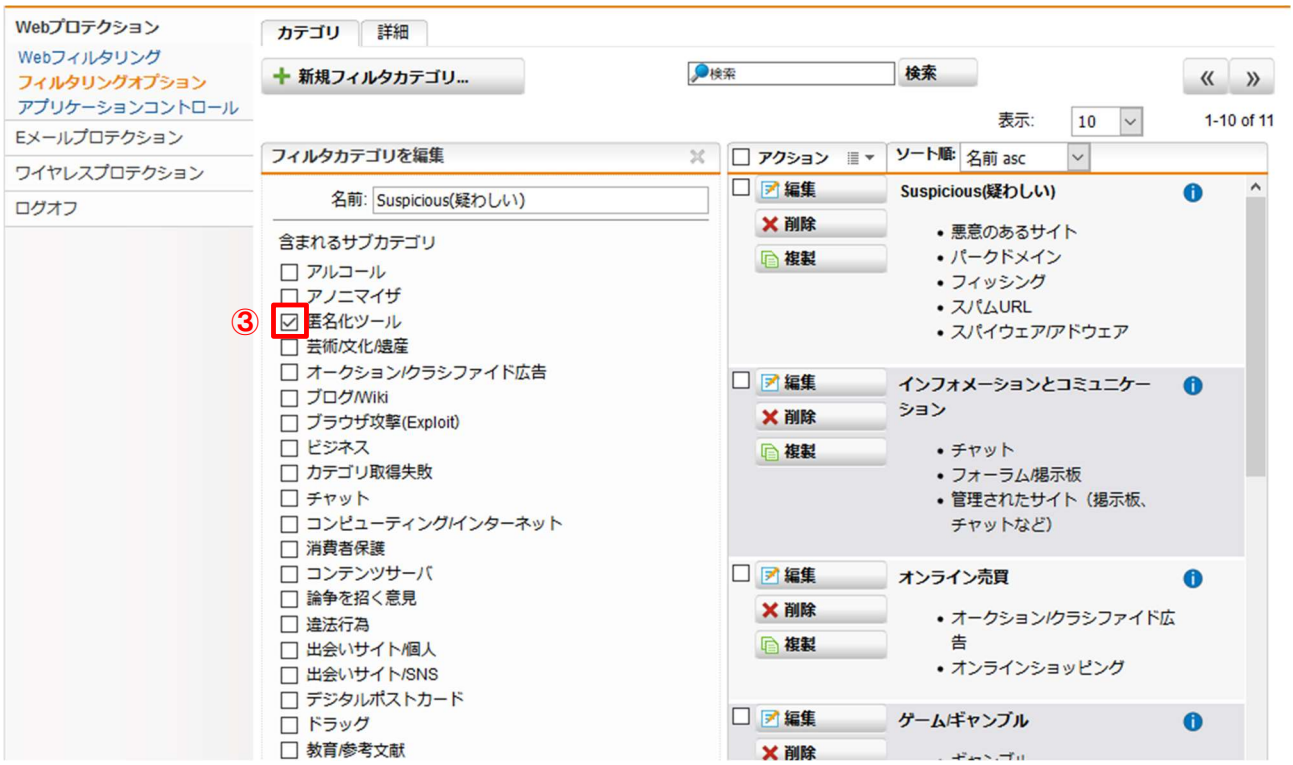
② 画面左側の「フィルタリングオプション」を押下すると、以下の画面「図：4-14-6 URLフィルタリングカテゴリー覧画面」が表示されるので、変更したいカテゴリの「編集」ボタンを押下する。



図：4-14-6 URLフィルタリングカテゴリー覧画面

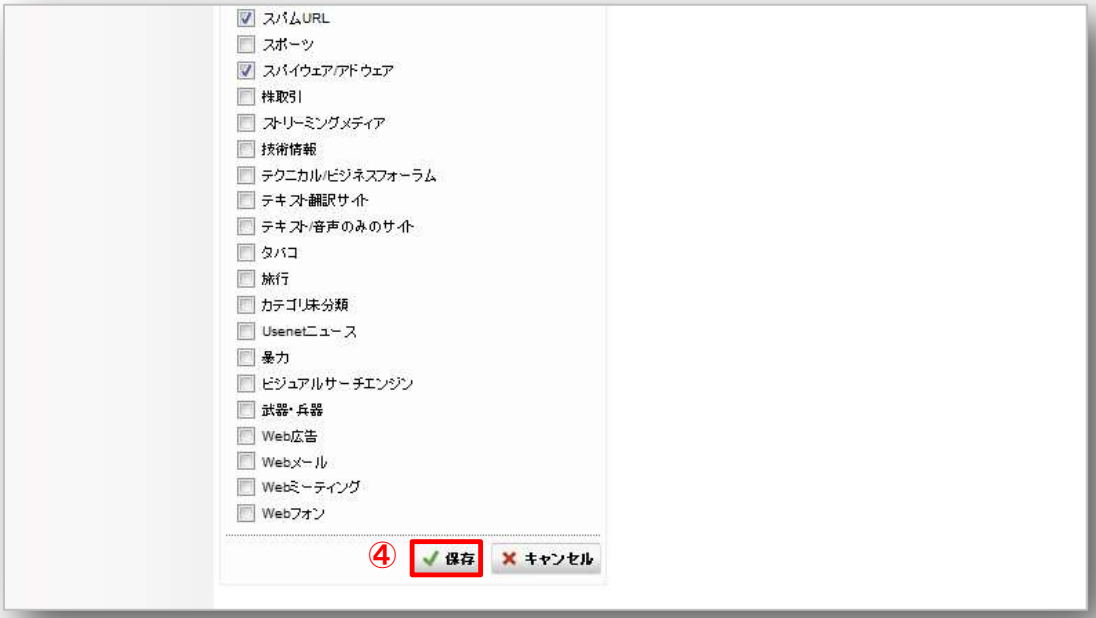
(注) 画面にはカテゴリが最大 10 エントリー表示されます。11 エントリー以降を確認する場合は、画面右上部に表示されている「>>」を押下し次頁を表示させてください。また、前ページに戻る場合は、同様に「<<」を押下してください。

③ 以下の画面「図：4-14-7 URL フィルタリングカテゴリ変更画面」が表示されるので、追加したいサブカテゴリのチェックボックスにチェックをいれる。



図：4-14-7 URL フィルタリングカテゴリ変更画面

④画面最下部にある「保存」ボタンを押下する。選択したカテゴリからはずしたいサブカテゴリがある場合は、チェックボックスからチェックをはずした後、同じく「保存」ボタンを押下する。



図：4-14-8 URL フィルタリングカテゴリ変更画面

⑤「図：4-14-9 URL フィルタリングカテゴリー覧画面」が表示されるので、選択したカテゴリに設定をしたサブカテゴリが追加されていることを確認する。

図：4-14-9 URL フィルタリングカテゴリー覧画面

■新しいURLカテゴリの作成
　URLカテゴリリストについて、お客さま任意の新しいカテゴリの作成、作成したカテゴリに任意のサブカテゴリを設定することができます。

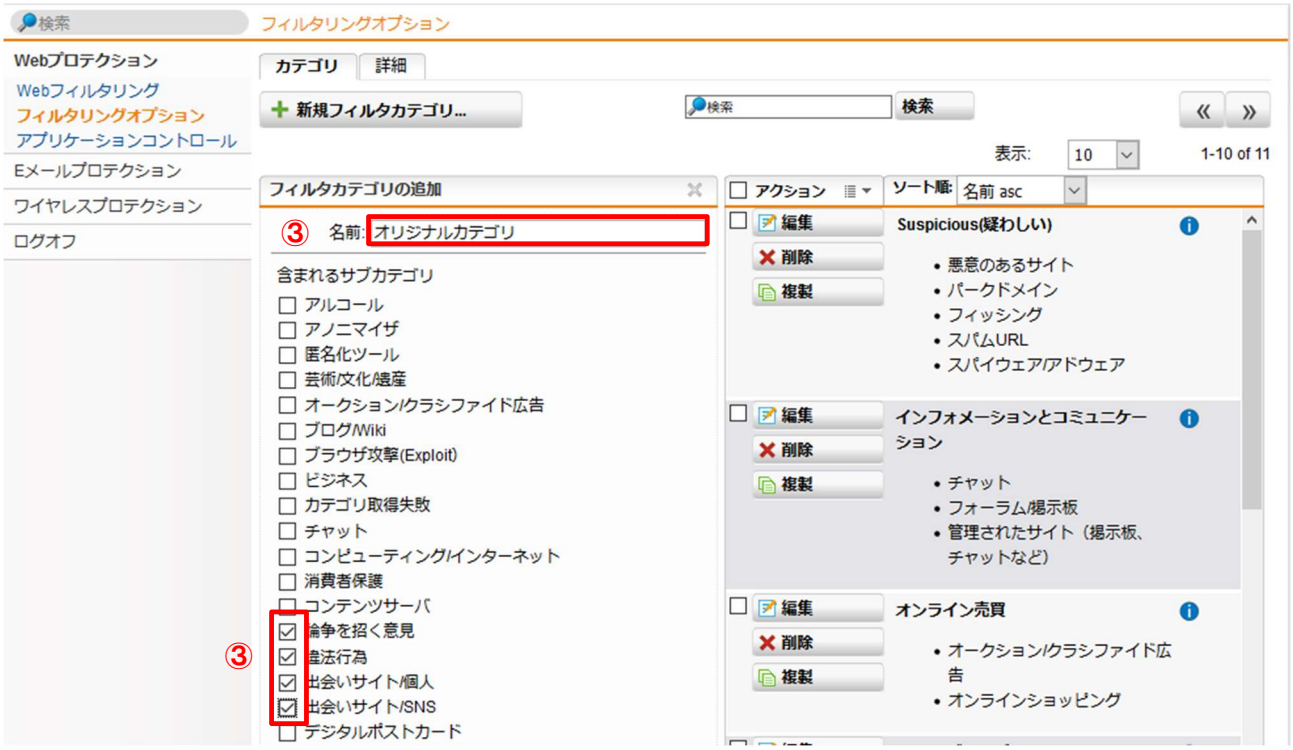
① ログインが成功すると、以下の画面「図：4-14-10 カスタマコントロール・ログイン直後画面」が表示されるので画面　左側の「Webプロテクション」を押下する。

図：4-14-10 カスタマコントロール・ログイン直後画面

② 画面左側の「フィルタリングオプション」を押下すると、以下の画面「図：4-14-11 URLフィルタリングカテゴリー覧画面」が表示されるので、「新規フィルタカテゴリ」ボタンを押下する。

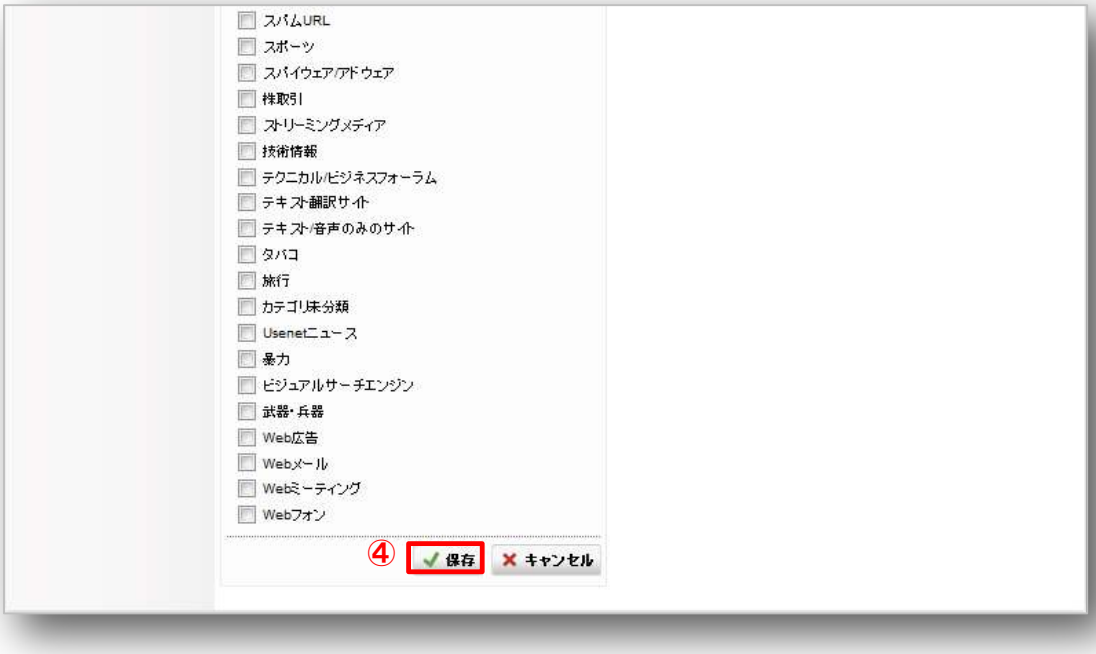
図：4-14-11 URL フィルタリングカテゴリー覧画面

③ 以下の画面「図：4-14-12 URL フィルタリングカテゴリ新規設定画面」が表示されるので、「名前」欄に任意のカテゴリ名称を入力し、そのカテゴリに含めたいサブカテゴリのチェックボックスにチェックをいれる。



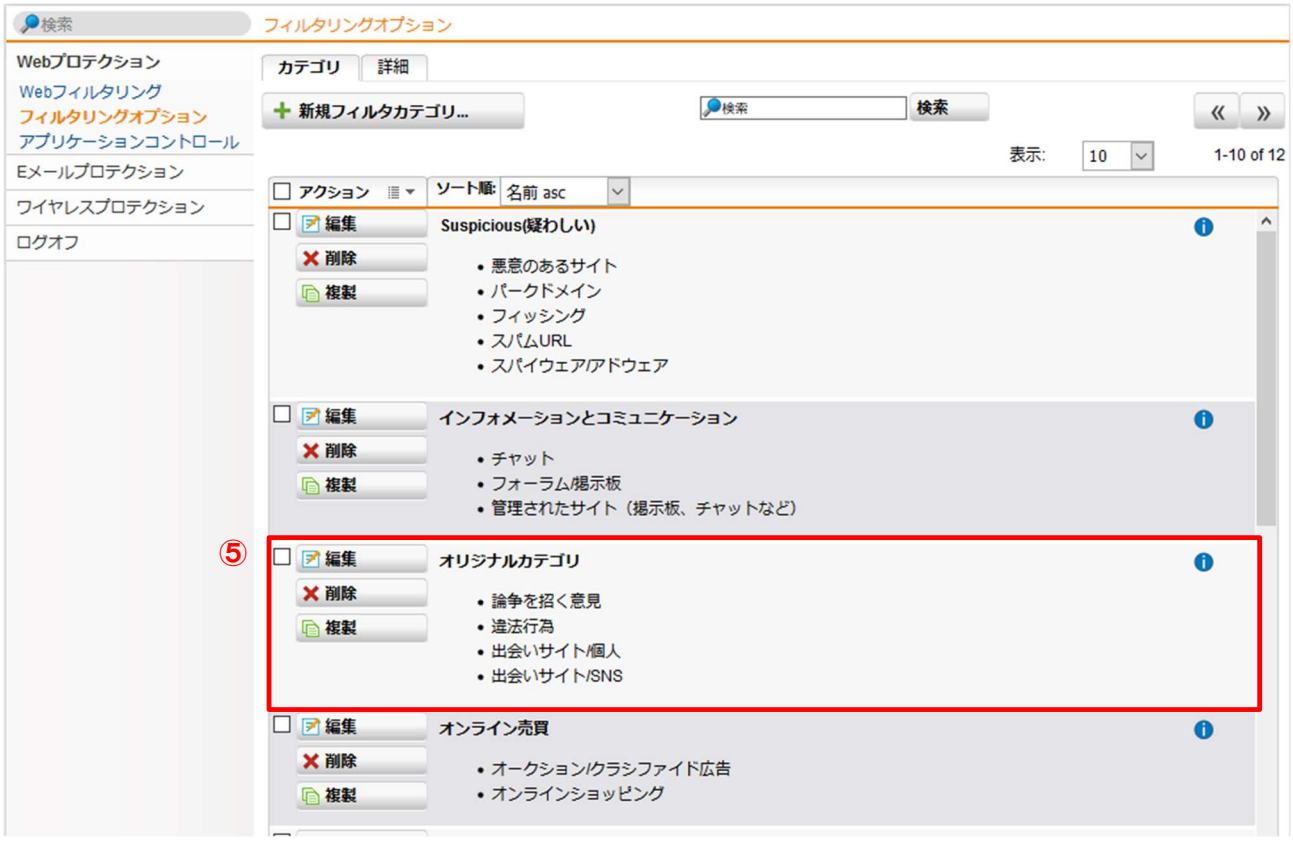
図：4-14-12 URL フィルタリングカテゴリ新規設定画面

④　画面最下にある「保存」ボタンを押下する。



図：4-14-13 URL フィルタリングカテゴリ新規設定画面

⑤ 「図：4-14-14 URLフィルタリングカテゴリー覧画面」が表示されるので、新しく作成したカテゴリが表示され、設定をしたサブカテゴリが含まれていることを確認する。



図：4-14-14 URL フィルタリングカテゴリー覧画面

■URLホワイト・ブラックリスト設定方法

① ログインが成功すると以下の画面「図：4-14-15 カスタマコントロール・ログイン直後画面」が表示されるので画面左側の「Webプロテクション」を押下する。

図：4-14-15 カスタマコントロール・ログイン直後画面

② 画面左側の「フィルタリングオプション」を押下すると、以下の画面「図：4-14-16 Web フィルタリング　ポリシー設定画面」が表示されるので、画面左側の「Default content filter action」を押下する。

図：4-14-16 Webフィルタリング　ポリシー設定画面

③ 以下の画面「図：4-14-17 フィルタアクションの編集画面」が表示されるので、画面上部の「Webサイト」アイコンを押下する。

図：4-14-17 フィルタアクションの編集画面

④ 以下の画面「図：4-14-18 URL ホワイト・ブラックリスト設定画面」が表示されるので、設定したい動作により、画面右側の「ブロックするサイト（ブラックリスト）」もしくは「許可するサイト（ホワイトリスト）」の「＋」アイコンのどちらかを押下する。

図：4-14-18 ホワイトリスト/ブラックリスト設定画面

⑤「＋」アイコンを押下すると新たな設定画面「図：4-14-19 ホワイトリスト/ブラックリスト追加画面」が表示される。

図：4-14-19 ホワイトリスト/ブラックリスト追加画面

⑥「名前」欄に適当な名前を入力する。「URLが次に合致」欄はプルダウンメニューより「正規表現」を選択する。「正規表現」欄の右側にある「＋」アイコンを押下し、ブラックリスト/ホワイトリストの対象としたいURLを入力する。入力後「適用」を押下する。

図:4-14-20 ホワイトリスト/ブラックリスト追加画面

(注)「図:4-14-20 ホワイトリスト/ブラックリスト追加画面」では、1つの「名前」に対して複数のドメイン入力が可能ですので、必要に応じて「＋」アイコンを再度押下してドメインを入力してください。

(注) 本設定でnttpc.co.jpを登録する場合、URLにnttpc.co.jpを含む全てのサイト(①www.nttpc.co.jp ②service.nttpc.co.jp ③www.nttpc.co.jp/product/imdex.html等)がブロックまたは通過の対象となります。意図しないサイトがブロックまたは通過されないようにご注意ください。

(注)"http://"の部分は登録しないようご注意ください。

⑦「コメント」欄に任意のコメントを入力して、最後に「保存」ボタンを押下する。

図:4-14-21 ホワイトリスト/ブラックリスト追加画面

⑧「保存」ボタンを押下すると、元の画面「図：4-14-21 URLカテゴリフィルタリング/URLホワイト・ブラックリスト設定画面」に戻るので、⑥で入力した「名前」が設定したどちらかに表示されていることを確認した後「保存」ボタンを押下する。

図：4-14-21 ホワイトリスト/ブラックリスト設定画面

（注）設定を解除したい場合は、設定した「名前」の左側にある「×」アイコンを押下し設定を削除後「保存」ボタンを押下してください。

（注）サービス初期設定として「ブロックするURLサイト（ブラックリスト）」に「Any domain expressions」が表示されています。本設定には弊社が指定したURLが複数登録されていますので絶対に削除しないでください。

（注）操作をしない時間が5分を超えた場合、自動的にログオフとなりますので、その際は再度ログインを行ってください。

4－15 WEB スキャンスキップリスト設定

本サービスで提供する「WEBアンチウイルス」では、お客さまの通信（HTTP/HTTPS）をゲートウェイ装置でプロキシ（代理応答）しスキャンすることにより実現しています。しかしながら、お客さまが使用されるアプリケーションの中にはゲートウェイ装置がプロキシ（代理応答）することを許可しないアプリケーションが存在しています。さらに、WEBカメラのような常時通信を行うことによりゲートウェイ装置の負荷を発生させ他の通信に影響を与える機器が存在しています。これらの通信先または通信元を登録することにより本問題を回避したい場合は、お客さまにて設定することが可能です。

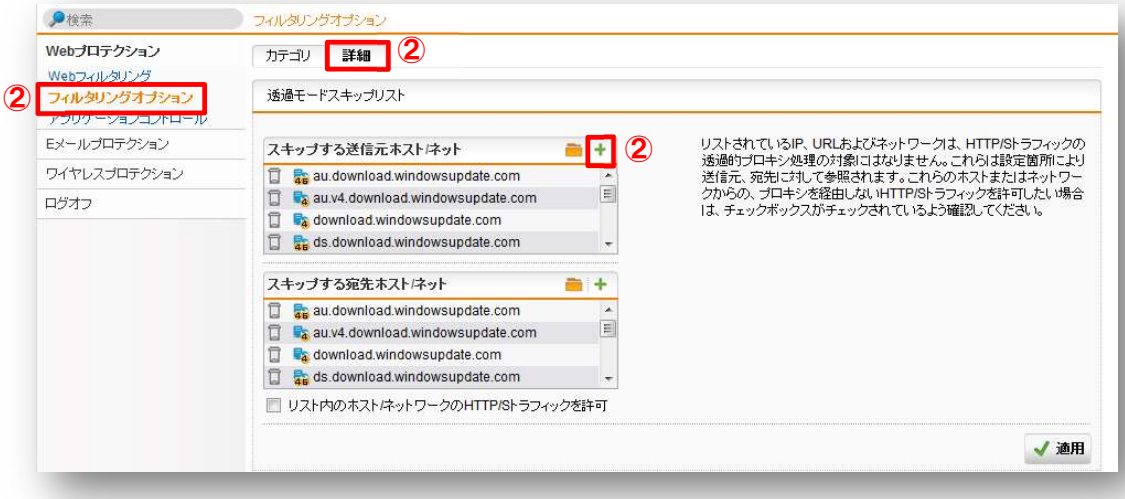
設定する操作手順は以下のとおりです。

■カスタマコントロール・ログイン方法
『4-11 カスタマコントロール・ログイン方法』をご参照ください。

■URLカテゴリフィルタ設定方法
①ログインが成功すると以下の画面「図：4-15-1 カスタマコントロール・ログイン直後画面」が表示されるので、画面左側の「Webプロテクション」を押下する。

図：4-15-1 カスタマコントロール・ログイン直後画面

②画面左側の「フィルタリングオプション」を押下後に画面上の「詳細」タブを押下すると、以下の画面「図：4-15-2 WEBスキャンスキップ（透過モードスキップリスト）設定画面①」が表示されるので、「スキップする送信元ホスト/ネット」欄にある「＋」アイコンを押下する。



図：4-15-2 WEBスキャンスキップ（透過モードスキップリスト）設定画面①

③「＋」アイコンを押下すると「図：4-15-3 ネットワークオブジェクトを追加設定画面」がポップアップ表示されるので、「名前」欄に適当な名前を入力する。「タイプ」欄はIPアドレス（例：192.168.0.10）で登録の場合「ホスト」、ドメイン（例：japan.co.jp）で登録の場合「DNSグループ」をプルダウンメニューより選択する。「タイプ」欄の選択により表示される「IPv4 アドレス」欄、または「ホスト名」欄にIPアドレスまたはドメインを入力した後、「保存」ボタンを押下する。

図：4-15-3 ネットワークオブジェクトを追加設定画面

④「保存」ボタンを押下すると元の画面「図：4-15-4 WEBスキャンスキップ（透過モードスキップリスト）設定画面②」に戻るので、「スキップする宛先ホスト/ネット」欄にある「フォルダ」アイコンを押下後、画面左側にネットワークの一覧が表示されるので、③で設定した「名前」と同一のものをドラッグ＆ドロップして「スキップする宛先ホスト/ネット」欄に設定する。

⑤「スキップする送信元ホスト/ネット」と「スキップする宛先ホスト/ネット」の両方に③で設定したものが表示されていることを確認した後「適用」ボタンを押下する。

図：4-15-4 WEBスキャンスキップ（透過モードスキップリスト）設定画面②

（注）本項で設定する対象機器は、一般的に送信と受信のどちらの通信も行うため、「スキップする送信元ホスト/ネット」と「スキップする宛先ホスト/ネット」の両方に同一設定を行わなかった場合、正常にスキャンスキップを行うことができなくなるためご注意ください。

（注）ゲートウェイ装置がプロキシ（代理応答）することを許可しないアプリケーションの通信先は、アプリケーションメーカより一般的には公開されていないためお客さま自身で特定することは困難です。同理由によりアプリケーションが使用できないことが疑われる場合はアプリケーション情報（名称・バージョン等）をご確認のうえSOCまでご連絡ください。

（注）操作をしない時間が5分を超えた場合、自動的にログオフとなりますので、その際はログインを行ってください。

4－16　アプリケーションコントロール設定

　本サービスで提供する「アプリケーションコントロール」により、ゲートウェイ装置配下からの特定アプリケーションでのアクセスを制限したい場合、お客さまにて設定することが可能です。

設定する操作手順は以下のとおりです。

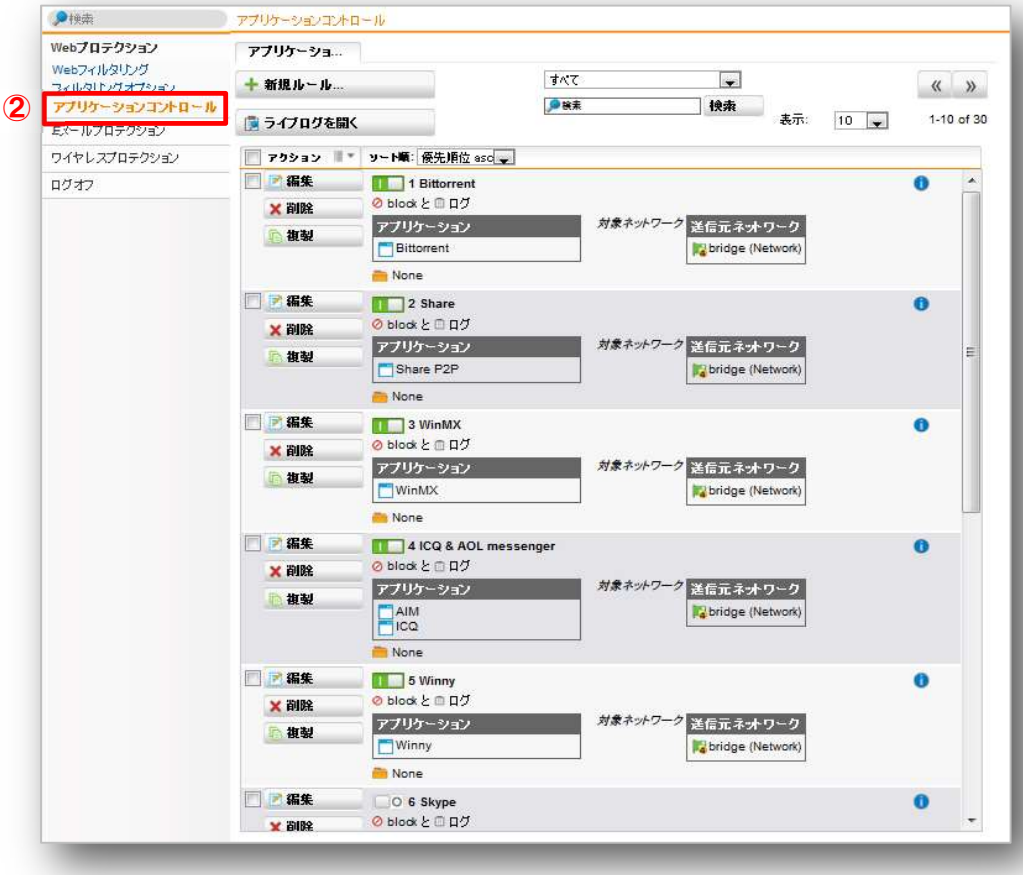
■カスタマコントロール・ログイン方法
『4-11　カスタマコントロール・ログイン方法』をご参照ください。

■アプリケーションコントロール設定の変更方法
①ログインが成功すると以下の画面「図：4-16-1 カスタマコントロール・ログイン直後画面」が表示されるので、画面左側の「Webプロテクション」を押下する。

図：4-16-1 カスタマコントロール・ログイン直後画面

②画面左側の「アプリケーションコントロール」を押下すると、以下の画面「図：4-16-2 アプリケーションコントロール一覧画面」が表示される。

（注）あらかじめサービス側で指定した 29 個のアプリケーションコントロールのエントリーが作成されており、アプリケーションの一部（P2P 系アプリケーション）は初期設定で有効（ブロック）となっています。



図：4-16-2 アプリケーションコントロール一覧画面

③現在設定されているアプリケーションコントロールを無効にしたい場合は、緑色のボタンを押下する。ボタンが灰色に変わると対象の設定は無効となる。

図：4-16-3 アプリケーションコントロール一覧詳細画面

④現在設定されているアプリケーションコントロールを有効にしたい場合は、灰色のボタンを押下する。ボタンが緑色に変わると対象の設定は有効となる。

図：4-16-4 アプリケーションコントロール一覧詳細画面

（注）あらかじめ設定されている29個のアプリケーションについては、有効または無効の設定のみ変更可能です。その他の設定内容の編集・変更や削除は行わないでください。

■新しいアプリケーションコントロールの設定の追加
あらかじめ設定されているアプリケーション以外について、ブロックを行いたいアプリケーションを新たにエントリーに追加することができます。

① ログインが成功すると以下の画面「図:4-16-5 カスタマコントロール・ログイン直後画面」が表示されるので画面左側の「Webプロテクション」を押下する。

図:4-16-5 カスタマコントロール・ログイン直後画面

② 画面左側の「アプリケーションコントロール」を押下すると、以下の画面「図:4-16-6アプリケーションコントロール一覧画面」が表示されるので、画面上部にある「新規ルール」ボタンを押下する。

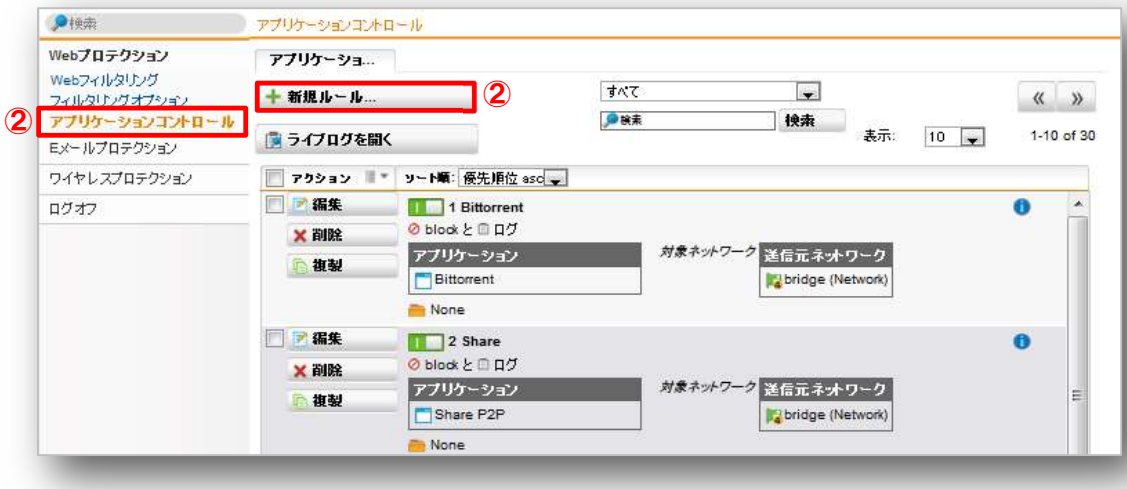
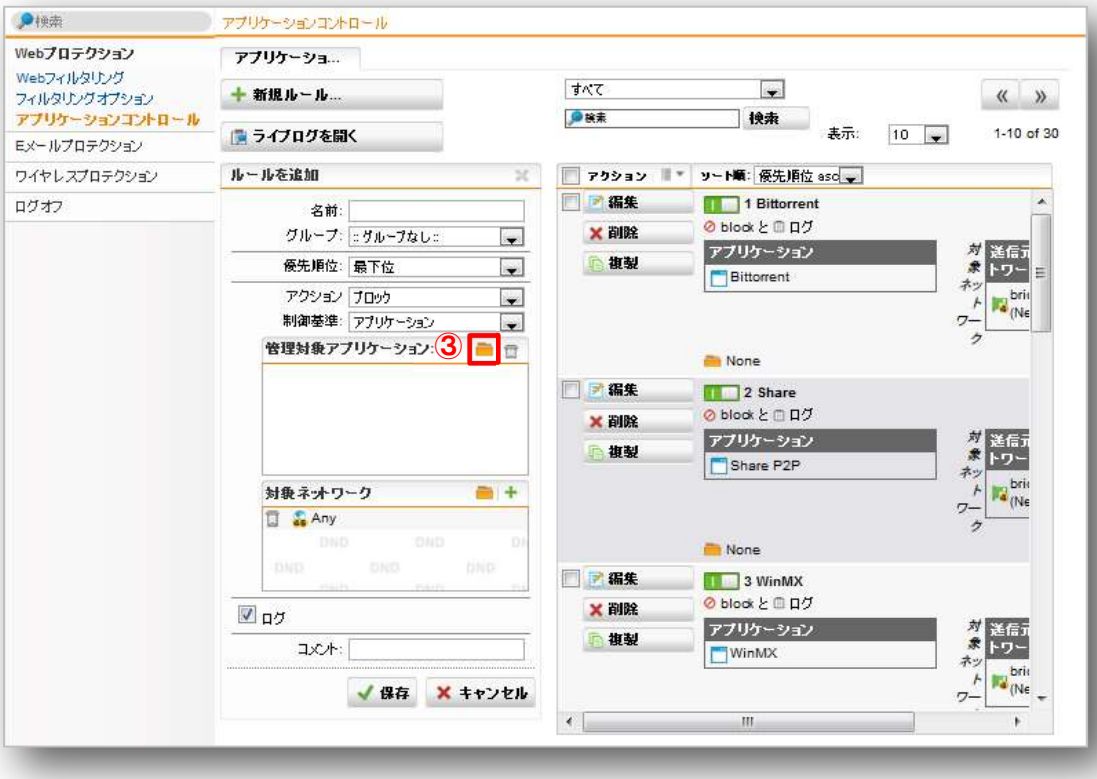


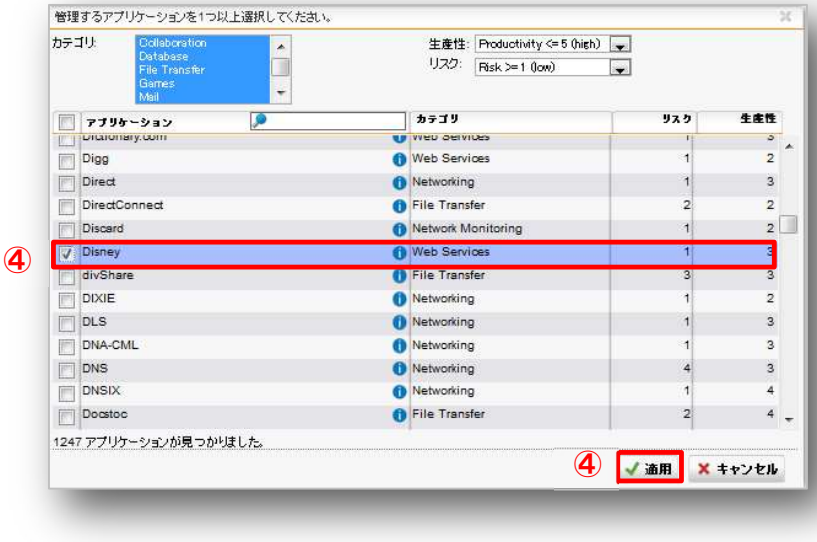
図:4-16-6 アプリケーションコントロール一覧画面

③ 以下の画面「図：4-16-7 アプリケーションコントロール新規設定画面」が表示されるので、「管理対象アプリケーション」の右側にあるフォルダアイコンを押下する。



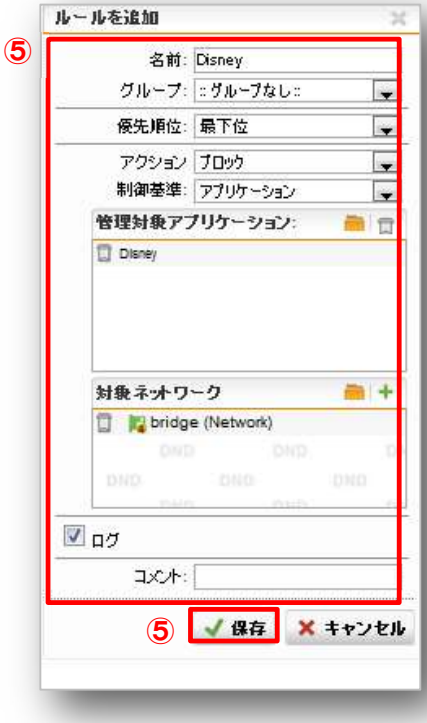
図：4-16-7 アプリケーションコントロール新規設定画面

④ 以下の画面「図：4-16-8 アプリケーションコントロール対象一覧画面」が表示されるので、ブロックを行いたいアプリケーションを検索し、チェックボックスにチェックを入れる。その後「適用」ボタンを押下する。



図：4-16-8 アプリケーションコントロール対象一覧画面

⑤ その他の設定項目については、下記の画面・情報に従って設定して「保存」ボタンを押下する。



【名前】
管理対象アプリケーションで選択したアプリケーションと同じ名前を入力

【グループ】
「グループなし」をそのまま選択

【優先順位】
「最下位」をそのまま選択
※画面の表示順を指し、アプリケーションコントロール機能の優劣ではありません

【アクション】
「ブロック」を指定するか、利用者への「警告」を表示するか選択

【制御基準】
「アプリケーション」をそのまま選択

【対象ネットワーク】
他のアプリケーションコントロールと同じネットワークを指定する
※次項⑥を参照

【ログ】
チェックが入ったままにする

【コメント】
任意で入力を行う

図：4-16-9 ルール追加画面

⑥　対象ネットワークを設定する。右側のフォルダアイコンを押下すると、画面左側にネットワークの一覧が表示される。ドラック&ドロップで、ネットワークを設定する。設定が完了したら、ネットワーク一覧上部の「×」アイコンを押下し、元のメニューに戻す。

（例）あらかじめエントリーのある 29 のアプリケーションコントロールに設定されているネットワークと同じものを必ず選択してください。通常は、「bridge (Network)」 のみです。

図：4-16-10 アプリケーションコントロール新規設定画面

⑦ 最後に「保存」ボタンを押下する。

図 4-16-11 ルール追加画面

⑧ 以下の画面「4-16-12 アプリケーションコントロール一覧画面」が表示されるので、画面右上の「>>」を押下し、画面の表示頁をすすめ、最終ページに、新たに定義したアプリケーションのエントリーがあることを確認する。また、有効/無効ボタンが緑の「有効」であることを確認する。

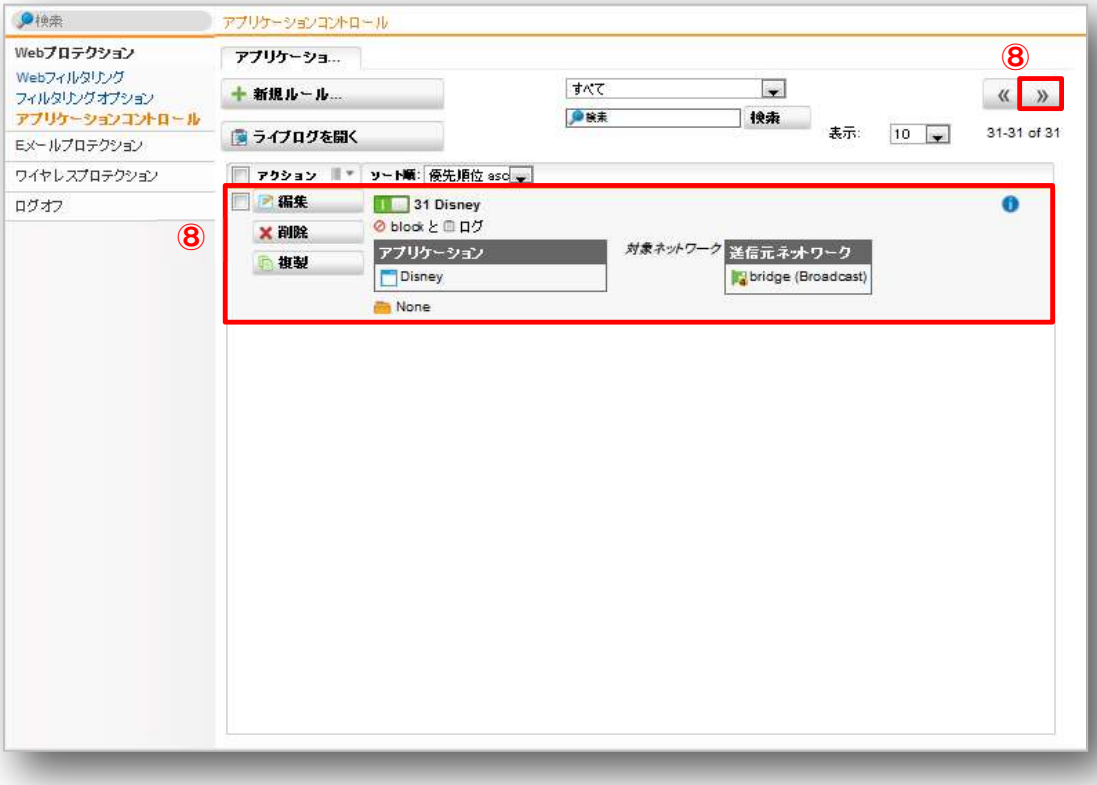


図:4-16-12 アプリケーションコントロール一覧画面

４－１７　WiFi アクセスポイント設定

　ゲートウェイ装置のWiFiアクセスポイント設定を有効にしたい場合、あるいはWiFiアクセスポイント設定を変更したい場合には、お客さまにて変更することが可能です。

（注）WiFiアクセスポイント設定を変更する場合、WiFi接続する端末の設定変更も必要となりますので、『４－９－３　端末の設定』に従って端末設定を実施の上、必ず接続確認を行ってください。また、ゲートウェイ装置に同梱されている「WiFi設定情報シート」（販路により同梱されていない場合があります。）、あるいはサービス開通時に「開通のご案内メール」にてお知らせしているWiFi設定情報が無効となりますので、設定変更を行う場合には必ずお客さまにて新しいWiFi設定情報を控えておいてください。

設定する操作手順は以下のとおりです。

■カスタマコントロール・ログイン方法
『４－１１　カスタマコントロール・ログイン方法』をご参照ください。

■WiFiアクセスポイントの有効化
①ログインが成功すると以下の画面「図：4-17-1 カスタマコントロール・ログイン直後画面」が表示されるので画面左側の「ワイヤレスプロテクション」を押下する。

図：4-17-1 カスタマコントロール・ログイン直後画面

②画面左側の「グローバル設定」を押下して、以下の画面が表示されたら右上のボタンを押下する。

（注）右上のボタンが緑色表示の場合は、すでにWiFiアクセスポイントは有効のため設定の必要はありませんので、WiFi接続する端末の設定（『４－９－３ 端末の設定』参照）のみを実施してください。

図：4-17-2 グローバル設定画面

③以下の画面が表示されるので、「許可インターフェース」の右側のフォルダアイコンを押下する。

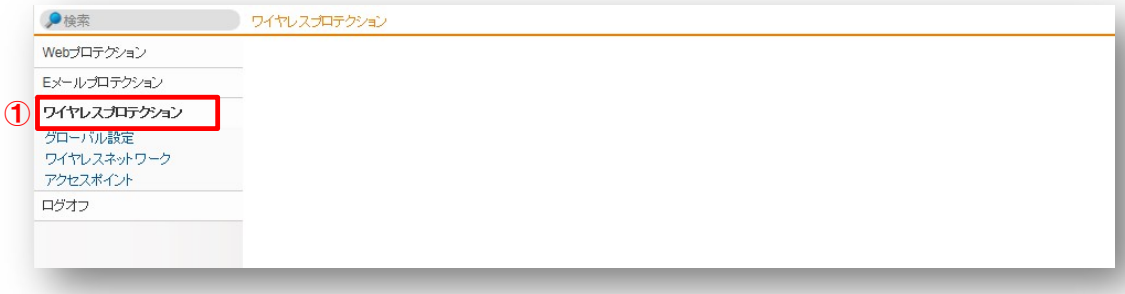
（注）「許可インターフェース」欄に「bridge」が設定されている場合は、すでに設定済みのため操作の必要はありませんので、WiFi接続する端末の設定（『４－９－３ 端末の設定』参照）のみを実施してください。

図：4-17-3 許可インターフェース設定画面

④画面左側にネットワークの一覧が表示されるので、「bridge」をドラッグ＆ドロップして「許可インターフェース」欄に設定して「適用」ボタンを押下する。画面右上のボタンが緑色に変わったことを確認する。

図：4-17-4 設定完了画面

■WiFiアクセスポイントの無効化
①ログインが成功すると以下の画面「図：4-17-5 カスタマコントロール・ログイン直後画面」が表示されるので、画面左側の「ワイヤレスプロテクション」を押下する。



図：4-17-5 カスタマコントロール・ログイン直後画面

②画面左側の「グローバル設定」を押下して、以下の画面が表示されたら右上のボタンを押下する。

図：4-17-6 グローバル設定画面

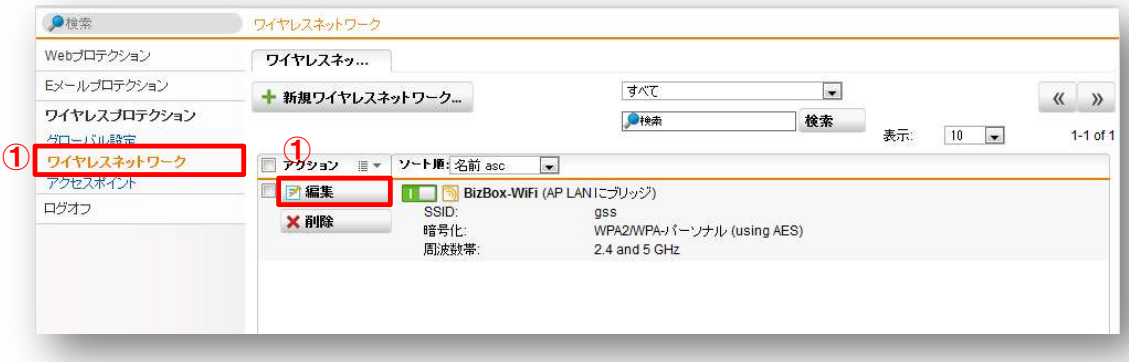
③画面右上のボタンを押下して、黄色に変わったことを確認した後「適用」ボタンを押下する。

図：4-17-7 グローバル設定画面

④画面右上のボタンが灰色に変わったことを確認する。

図：4-17-8 設定完了画面

■WiFi設定情報の変更（SSID/パスフレーズの変更）
①画面左側の「ワイヤレスネットワーク」を押下して以下の画面を表示させたあと、「編集」ボタンを押下する。



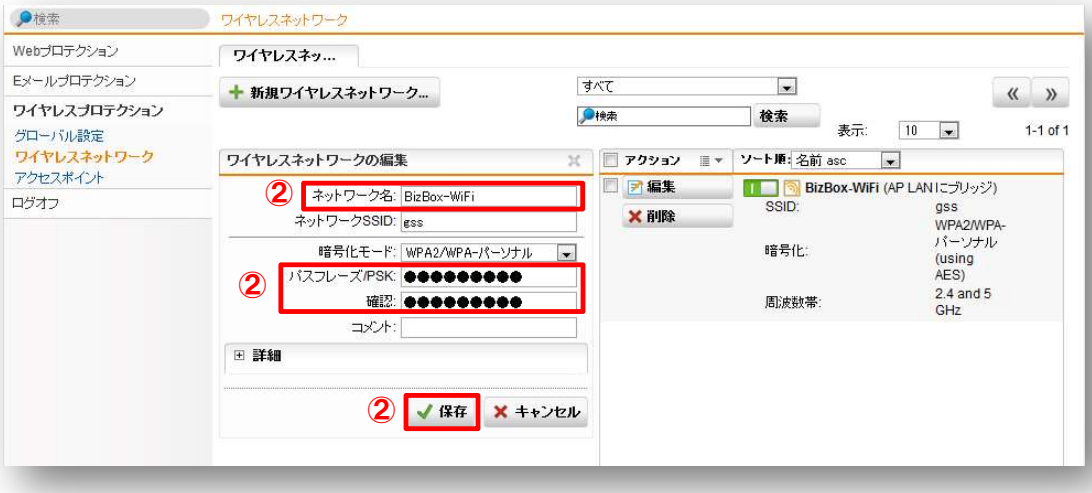
図：4-17-9 ワイヤレスネットワーク設定画面

②「ネットワークSSID」欄に新しいSSIDを入力する。また「パスフレーズ/PSK」欄および「確認」欄に新しいパスフレーズキーを入力する。入力が完了したら、「保存」ボタンを押下する。

（注）「ネットワークSSID」として設定できる文字は1～32文字までの英数字および記号です。カンマは使用できません。
また、先頭または末尾にスペースを入れることはできません。

（注）「パスフレーズ/PSK」と「確認」の欄は同一の文字を入力してください。パスフレーズとして設定できる文字は、8～63文字までの英数字および記号です。

（注）「ネットワークSSID」、「パスフレーズ/PSK」、「確認」以外の欄は絶対に変更や削除をしないでください。



図：4-17-10 ワイヤレスネットワーク編集画面

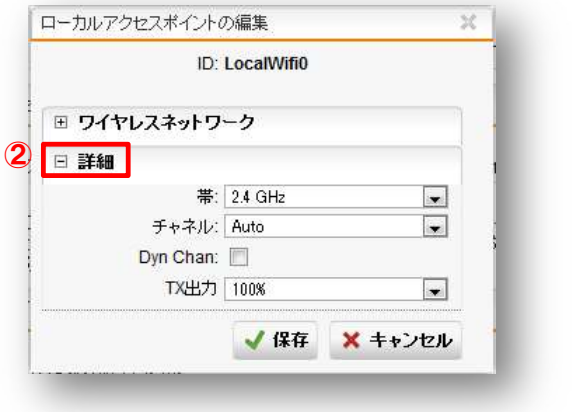
③設定を有効にするため、「ワイヤレスネットワーク」の画面中央のスイッチを押下して灰色になったことを確認したあと、再びスイッチを押下して緑色に変わったことを確認する。

図：4-17-11 ワイヤレスネットワーク設定画面

■WiFi設定情報の変更（周波数帯/チャネルの変更）
①画面左側の「アクセスポイント」を押下して以下の画面を表示させたあと、「編集」を押下する。

図：4-17-12 アクセスポイント設定画面

②「詳細」の左側にある「＋」を押下する。



図：4-17-13 アクセスポイント編集画面

③「帯」の右側にある「▼」を押下し、「2.4GHz」または「5GHz」を選択する。

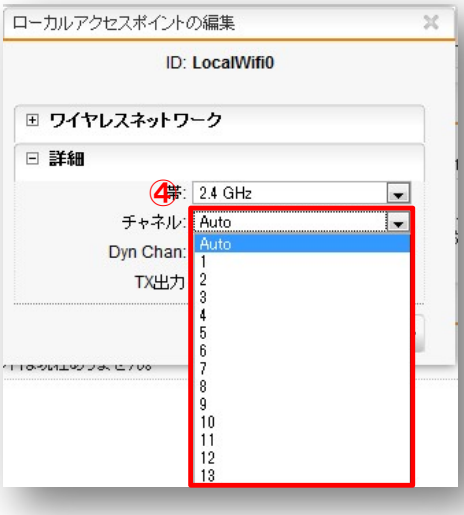
(注) WiFi接続する端末が11b/11g/11n対応の場合は「2.4GHz」を、11a/11n対応の場合は「5GHz」を選択してください。

(注) ※「2.4GHz」と「5GHz」を併用することはできません。1台でも「2.4GHz」対応の端末が存在する場合には「2.4GHz」を選択してください。

図：4-17-14 周波数帯設定画面

④「チャネル」の右側にある「▼」を押下し、利用するチャネルを選択する。選択が完了したら「保存」を押下する。

（注）初期設定および推奨設定は「Auto」です。ゲートウェイ装置は電波環境をチェックして自動的にチャネルを設定しますので、特に問題が無い限り「Auto」のままでご利用ください。



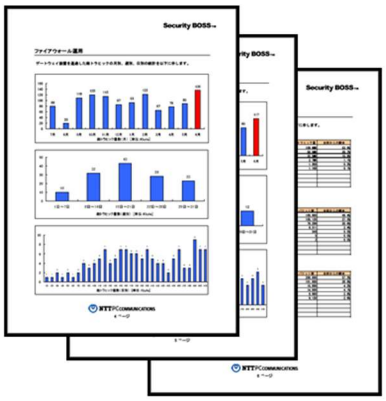
図：4-18-15　チャネル設定画面

4－18 月次レポート

すべてのご契約者さまを対象に、月に1度ゲートウェイ装置の運用レポートを作成します。運用レポートは、ポータルサイトよりダウンロードし、閲覧してください。(『5 ユーザ・サポート・サイト』 参照) 月次レポートの内容は以下のとおりです。

【活動報告書】
ゲートウェイ装置にて処理をおこなった集計の一覧になります。
ゲートウェイ装置の機能についての詳細な動作状況を確認することができます。
サービスが正常に稼動していることをご確認ください。

ファイアウォール運用

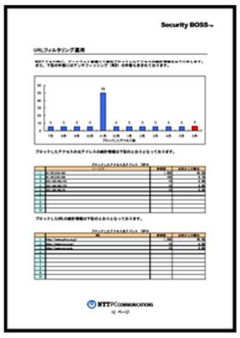


メールアンチウイルス運用

WEBアンチウイルス運用

メールアンチスパム運用

URLフィルタリング運用



※アンチスパム機能にて、検知されたスパムメールの宛先に複数のメールアドレスが含まれている場合や、メーリングリスト用メールアドレスが含まれている場合でも同一メールは1件とカウントしています。

※アンチスパム機能にて、警告設定 (検知されたスパムメールをゲートウェイ装置内に隔離せずにEメールの件名に*SPAM*タグを付与) を選択した場合は、月次レポートにカウントされません。

※FTP通信によるウィルス検知については、Webアンチウィルス欄にカウントされます。

4－19 ゲートウェイ装置の停止/起動

お客さま宅内の法定点検等により、ゲートウェイ装置の運用を中断する場合、当社からの監視サービスを一時的に停止する必要がございますので、電源をOFFする場合は事前にSOCまでご連絡ください。

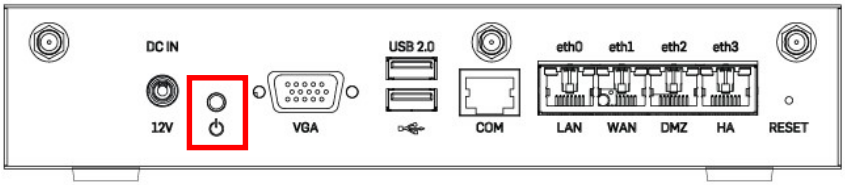
Eメール連絡先、電話連絡先については『7－1　お問い合わせ方法』をご参照ください。

4－19－1 停止手順

以下の手順でゲートウェイ装置の停止をおこなうことができます。

① Biz Box UTM「SSB」「5」の場合

［手順1］装置背面の「電源スイッチ（Power）」が青く点灯していることを確認し、「電源スイッチ（Power）」を短く（1秒以内）押します



図：4-19-1 ゲートウェイ装置停止

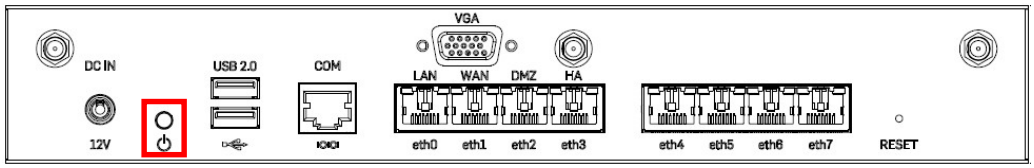
（注）『電源スイッチ（Power）』を長押し（1秒以上）しますと強制電源断による終了となりますのでSOCから依頼のあったとき以外は行わないでください。

［手順2］約30秒後に「電源スイッチ（Power）」が赤い点灯に変わっていることを確認し、電源コンセントを抜いてください。

（電源停止完了）

② Biz Box UTM「SSB」「Standard／Professional」の場合

［手順 1］装置背面の「電源スイッチ（Power）」が青く点灯していることを確認し、「電源スイッチ（Power）」を短く（1 秒以内）押します。



図：4-19-2 ゲートウェイ装置停止

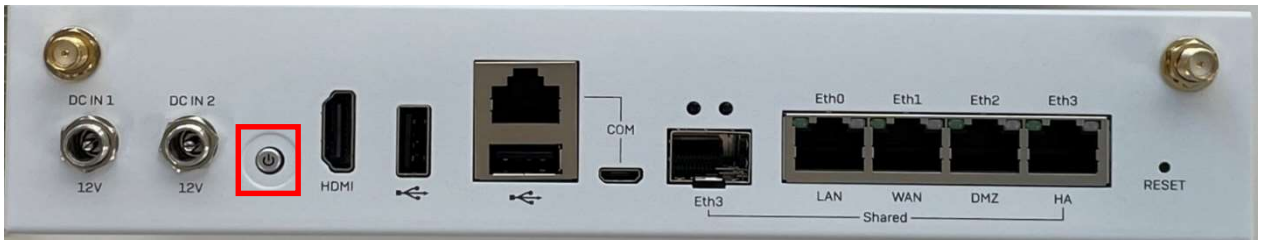
（注）『電源スイッチ（Power）』を長押し（1秒以上）しますと強制電源断による終了となりますのでSOCから依頼のあったとき以外は行わないでください。

［手順2］約30秒後に「電源スイッチ（Power）」が赤い点灯に変わっていることを確認し、電源コンセントを抜いてください。

（電源停止完了）

③　Biz Box UTM「SG105w rev3」の場合

［手順1］装置背面の「電源スイッチ（Power）」が青く点灯していることを確認し、「電源スイッチ（Power）」を短く（1秒以内）押します



図：4-19-3　ゲートウェイ装置停止

（注）『電源スイッチ（Power）』を長押し（1秒以上）しますと強制電源断による終了となりますのでSOCから依頼のあったとき以外は行わないでください。

［手順2］約30秒後に「電源スイッチ（Power）」が赤い点灯に変わっていることを確認し、電源コンセントを抜いてください。

（電源停止完了）

④　Biz Box UTM「SG125w rev3」の場合

［手順1］装置背面の「電源スイッチ（Power）」が青く点灯していることを確認し、「電源スイッチ（Power）」を短く（1秒以内）押します

図：4-19-4　ゲートウェイ装置停止

（注）『電源スイッチ（Power）』を長押し（1秒以上）しますと強制電源断による終了となりますのでSOCから依頼のあったとき以外は行わないでください。

［手順2］約30秒後に「電源スイッチ（Power）」が赤い点灯に変わっていることを確認し、電源コンセントを抜いてください。

（電源停止完了）

4－19－2 起動手順

以下の手順でゲートウェイ装置の起動をおこなうことができます。

① Biz Box UTM「SSB」「5」の場合

［手順1］装置背面の「電源スイッチ（Power）」を確認してください。
赤く点灯している場合：「電源スイッチ（Power）」を押してください。
青く点灯している場合： 何にもせず［手順2］へ進んでください。

（注）通常は電源コンセントを接続した時点で起動しますので、ボタン操作は必要ありません。上記操作は電源を停止した後も通電状態のままであった時のみに実施する操作手順となります。

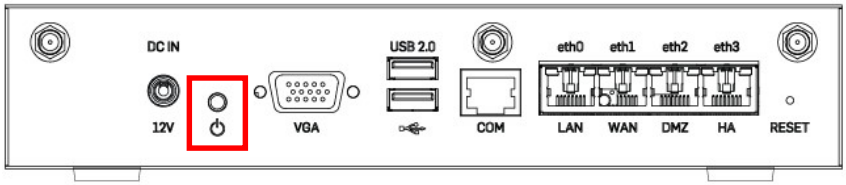


図4-19-5 ゲートウェイ装置起動

［手順2］「電源スイッチ（Power）」が青く点灯します。

［手順3］約2分経過したら起動の完了です。

（電源起動完了）

② Biz Box UTM「SSB」「Standard／Professional」の場合

［手順1］装置背面の「電源スイッチ（Power）」を確認してください。
赤く点灯している場合：「電源スイッチ（Power）」を押してください。
青く点灯している場合： 何にもせず［手順2］へ進んでください。

（注）通常は電源コンセントを接続した時点で起動しますので、ボタン操作は必要ありません。上記操作は電源を停止した後も通電状態のままであった時のみに実施する操作手順となります。

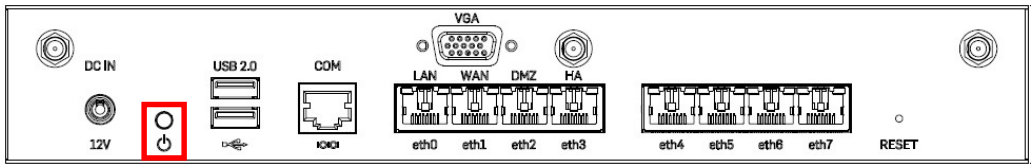


図4-19-6 ゲートウェイ装置起動

［手順2］「電源スイッチ（Power）」が青く点灯します。

［手順3］約2分経過したら起動の完了です。

（電源起動完了）

③ Biz Box UTM 「SG105w rev3」の場合

［手順1］装置背面の「電源スイッチ（Power）」を確認してください。
赤く点灯している場合：「電源スイッチ（Power）」を押してください。
青く点灯している場合： 何にもせず［手順2］へ進んでください。

（注）通常は電源コンセントを接続した時点で起動しますので、ボタン操作は必要ありません。上記操作は電源を停止した後も通電状態のままであった時のみに実施する操作手順となります。

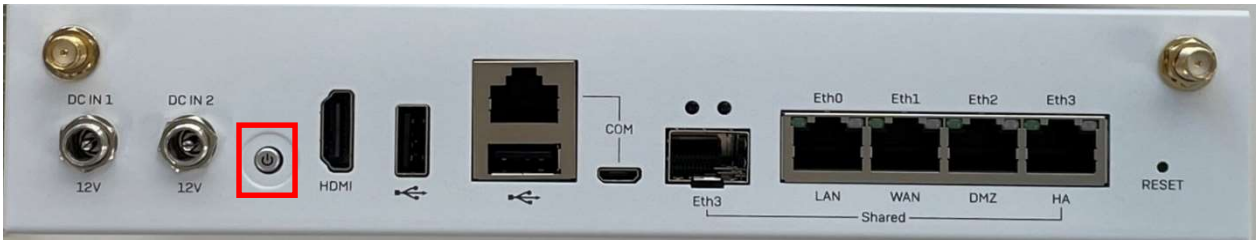


図4-19-7 ゲートウェイ装置起動

［手順2］「電源スイッチ（Power）」が青く点灯します。

［手順3］約2分経過したら起動の完了です。

（電源起動完了）

④ Biz Box UTM 「SG125w rev3」の場合

［手順1］装置背面の「電源スイッチ（Power）」を確認してください。
赤く点灯している場合：「電源スイッチ（Power）」を押してください。
青く点灯している場合： 何にもせず［手順2］へ進んでください。

（注）通常は電源コンセントを接続した時点で起動しますので、ボタン操作は必要ありません。上記操作は電源を停止した後も通電状態のままであった時のみに実施する操作手順となります。

図4-19-8 ゲートウェイ装置起動

［手順2］「電源スイッチ（Power）」が青く点灯します。

［手順3］約2分経過したら起動の完了です。

（電源起動完了）

４－20 運用時の注意事項

① 電源をOFFする場合はSOCまでご連絡ください。
当社のSOCにて、お客さま宅内に設置しておりますゲートウェイ装置の監視をおこなっております。お客さまにて予告無く電源の停止をされますと、SOCにて故障であると誤検知してしまいます。

② 添付品保管のお願い
お客さま宅内に設置しましたゲートウェイ装置に付属している添付品、および梱包用の箱は返却や保守交換の際に必要になりますので、大切に保管してください。

③ ゲートウェイ装置設置場所の移動
ゲートウェイ装置を設置した場所から移動する際は、SOCへご連絡ください（『６－１　お問い合わせ方法参照』）。
場合によって、当社の派遣する作業員による現地工事（有償）が発生する場合がございます。

5. ユーザ・サポート・サイト

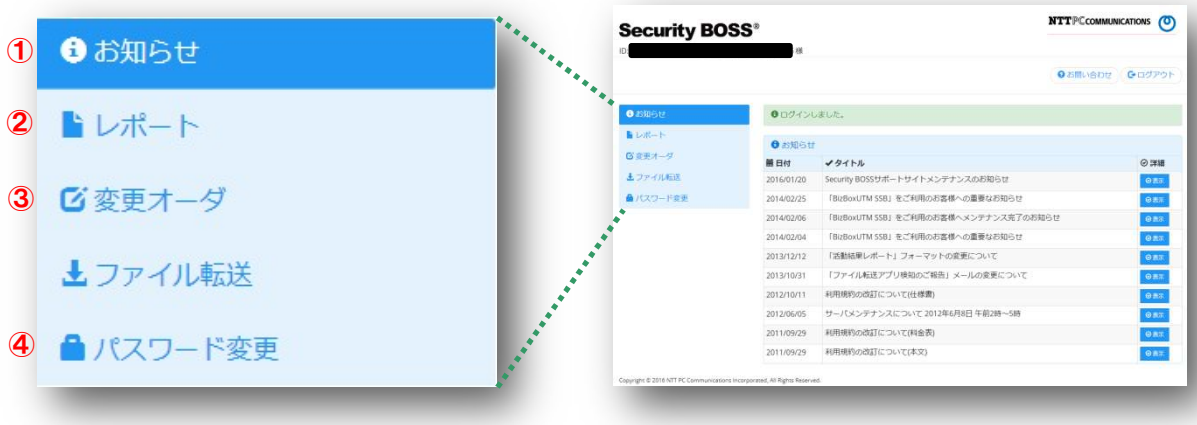
ご契約の管理者さまが操作をおこなえるポータルサイトです。このサイトでは以下の操作をおこなうことができます。ユーザ・サポート・サイトへは、管理者の方のみがログインをおこなうようにしてください。

① お知らせ
本サービスにおける当社からの新しい情報が表示されます。定期的に確認してください。

② レポート
過去1年分の月次対応レポートをダウンロードすることができます。
月次対応レポートについては、『4-18 月次レポート』をご参照ください。

③ サポート
③-1 サービス内容の変更をおこないたい場合、ご希望の設定を記載した設定変更表のアップロードをおこなうことができます。
③-2 SecurityBOSSを利用する際のアプリケーションをダウンロードすることができます。
③-3 お客さまが希望された場合の特定のデータをダウンロードする際に使用します。

④ ログインパスワードの変更
ログインパスワードの変更をおこなうことができます。

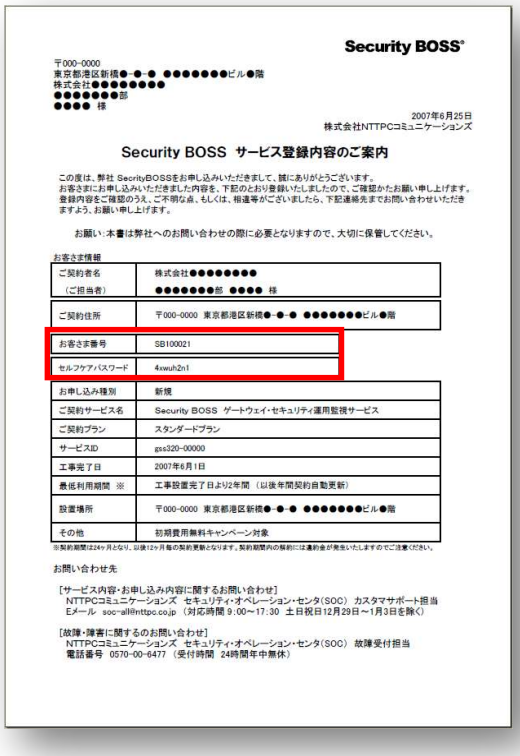


図：5－1 ユーザ・サポート・サイトのTOP画面

5－1 ログイン

ユーザ・サポート・サイトへアクセスをおこないます。以下の手順を実施してください。

［手順1］ログインID、パスワードの確認
『Security BOSSサービス登録内容のご案内』を確認してください。
『お客さま番号』 → ログインID
『セルフケアパスワード』 → パスワード
となります。



Security BOSS®

〒000-0000
東京都港区新橋●-●-● ●●●●●●●●ビル●階
株式会社●●●●●●●●●
●●●●●●●部
●●●● 様

2007年6月25日
株式会社NTTPCコミュニケーションズ

Security BOSS サービス登録内容のご案内

この度は、弊社 SecrityBOSSをお申し込みいただきまして、誠にありがとうございます。
お客さまにお申し込みいただきました内容を、下記のとおり登録いたしましたので、ご確認かたお願い申し上げます。
登録内容をご確認のうえ、ご不明な点、もしくは、相違等がございましたら、下記連絡先までお問い合わせいただきますよう、お願い申し上げます。

お願い：本書は弊社へのお問い合わせの際に必要となりますので、大切に保管してください。

お客さま情報

ご契約者名（ご担当者）	株式会社●●●●●●●● ●●●●●●●部 ●●●● 様
ご契約住所	〒000-0000 東京都港区新橋●-●-● ●●●●●●●●ビル●階
お客さま番号	SB100021
セルフケアパスワード	4xwuh2n1
お申し込み種別	新規
ご契約サービス名	Security BOSS ゲートウェイ・セキュリティ運用監視サービス
ご契約プラン	スタンダードプラン
サービスID	gss320-00000
工事完了日	2007年6月1日
最低利用期間 ※	工事設置完了日より2年間（以後年間契約自動更新）
設置場所	〒000-0000 東京都港区新橋●-●-● ●●●●●●●●ビル●階
その他	初期費用無料キャンペーン対象

※契約期間は24ヶ月となり、以後12ヶ月毎の契約更新となります。契約期間内の解約には違約金が発生いたしますのでご注意ください。

お問い合わせ先

［サービス内容・お申し込み内容に関するお問い合わせ］
NTTPCコミュニケーションズ セキュリティ・オペレーション・センタ（SOC） カスタマサポート担当
Eメール soc-all@nttpc.co.jp （対応時間 9:00～17:30 土日祝日12月29日～1月3日を除く）

［故障・障害に関するお問い合わせ］
NTTPCコミュニケーションズ セキュリティ・オペレーション・センタ（SOC） 故障受付担当
電話番号 0570-00-6477 （受付時間 24時間年中無休）

図：5-1-1『Security BOSSサービス登録内容のご案内』

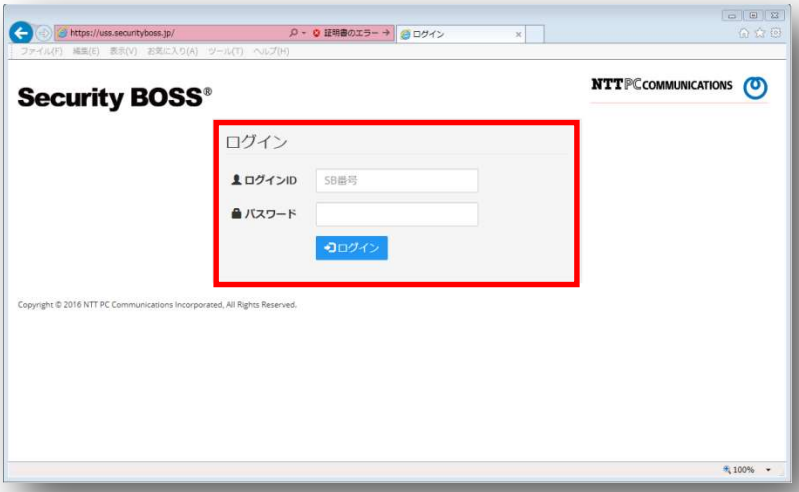
［手順2］サイトへアクセス
ブラウザのアドレスバーにアドレスを入力し、移動を押下してください。

【URL】https://uss.securityboss.jp

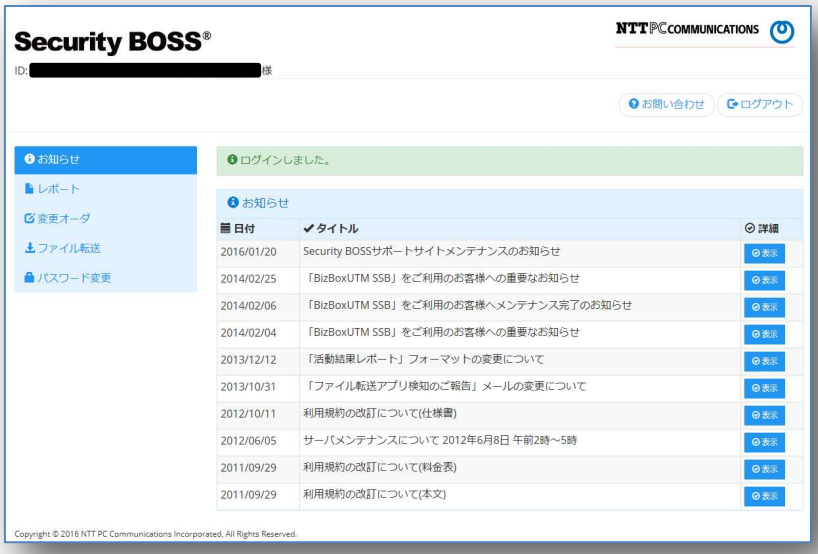
図：5-1-2 アドレスの入力

［手順３］ログイン

ログインIDにお客さま番号、パスワードにセルフケアパスワードを入力し、『ログイン』を押下してください。
お知らせ』の画面が表示されたら、ログイン完了です。



図：5-1-3 アカウント情報の入力



図：5-1-4 ログイン完了

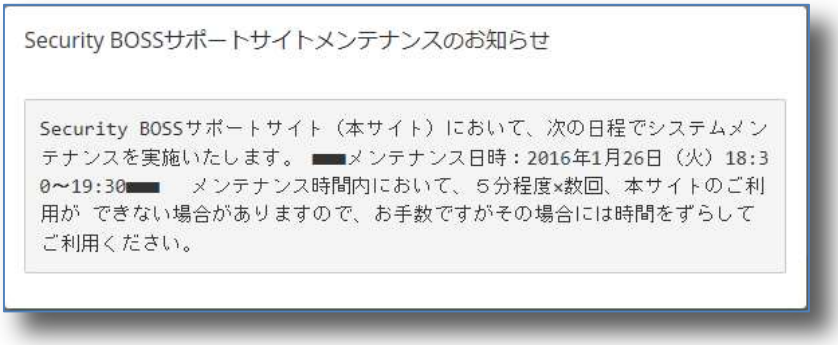
（注）パスワードとして使用するセルフケアパスワードは、お客さまご自身で定期的に変更をしていただく必要があります。
詳しくは『５－５　ログインパスワードの変更』をご確認ください。

5－2 お知らせの確認

［手順1］お知らせを表示させる
画面左のメニューの中から『お知らせ』を押下してください。
“お知らせ”が表示されます。

図：5-2-1 お知らせの表示

［手順2］詳細内容の表示
詳細を確認したいお知らせの「表示」ボタンをクリックするとお知らせの詳細が表示されます。



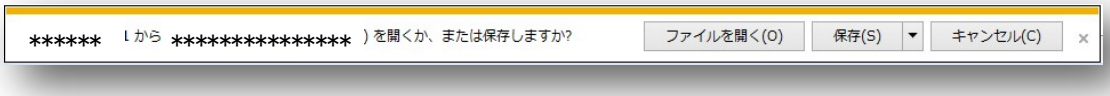
図：5-2-2 お知らせの詳細

5－3 月次レポートのダウンロード

［手順1］月次レポートの表示
画面左のメニューから『レポート』を押下してください。

図：5-3-1 レポートを選択

［手順2］月次レポートのダウンロード
月次レポートの「ファイル一覧」ボタンを押下すると、ダウンロードできるレポート情報が表示されます。閲覧したいレポートの「ダウンロード」ボタンを押下すると、レポートファイルをダウンロードすることができます。



図：5-3-2 月次レポートのダウンロード

■ 月次レポート
ゲートウェイ装置にておこなったセキュリティ処理の集計一覧です。
ゲートウェイ装置のセキュリティ機能について、詳細な動作状況を確認することができます。
【更新】 1回/月

■ 設定内容表
お客さまに提供しているサービスの設定一覧を確認することができます。
設定を変更したい場合、記入用紙としても使用します。
設定内容表は、お客さまからの申請等でゲートウェイ装置に設定変更をおこなった場合、その都度更新されます。
現在の設定内容を確認する際や、設定を変更したい場合に活用してください。
【更新】 随時

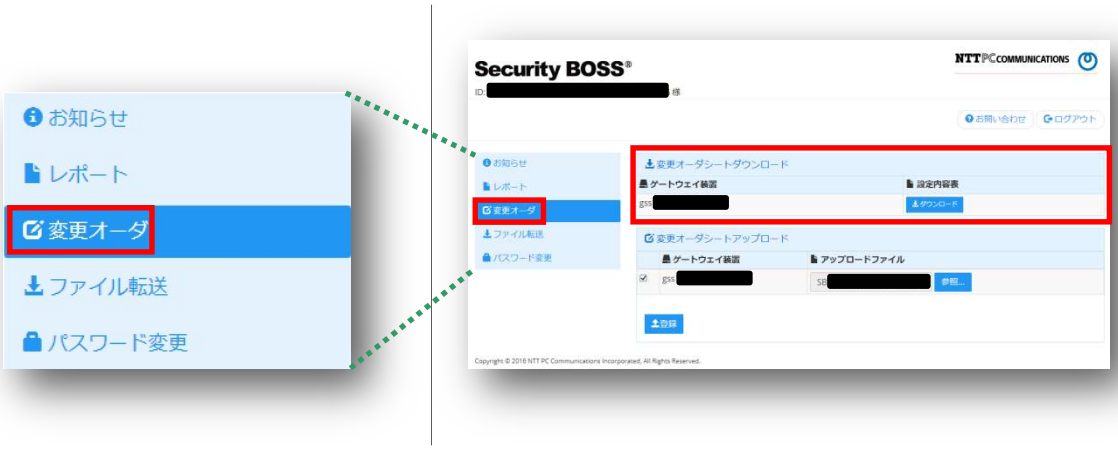
5－4 サービス内容の変更

［手順1］変更オーダシートのダウンロード

現在の最新の設定内容が記載されている『変更オーダシート』を、ユーザ・サポート・サイトからダウンロードします。画面左のメニューから『変更オーダ』を押下してください。

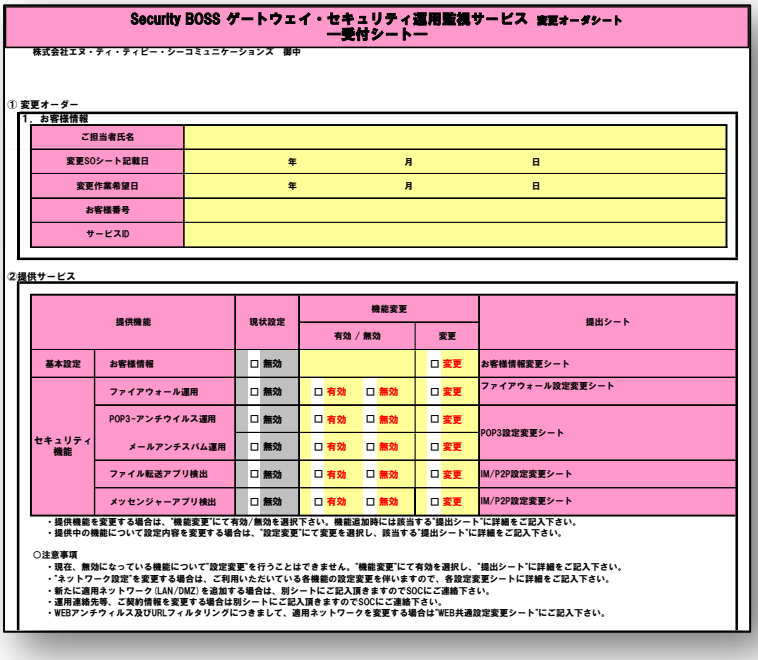
画面に『変更オーダシートダウンロード』画面が表示されますので、「ダウンロード」ボタンを押下して『変更オーダシート』ファイルをダウンロードしてください。

※『5－3 月次レポートのダウンロード』の手順で、『設定内容表』を押下し、『変更オーダシート』をダウンロードすることも可能です。



図：5-4-1 変更オーダシートのダウンロード画面

変更オーダシートに記載されているお客さまの現在の設定を確認してください。



Security BOSS ゲートウェイ・セキュリティ運用監視サービス 変更オーダシート
―受付シート―

株式会社エヌ・ティ・ティピー・シーコミュニケーションズ 御中

① 変更オーダー

1. お客様情報

ご担当者氏名	
変更SOシート記載日	年 月 日
変更作業希望日	年 月 日
お客様番号	
サービスID	

②提供サービス

提供機能		現状設定	機能変更		提出シート
			有効 / 無効	変更	
基本設定	お客様情報	□ 無効		□ 変更	お客様情報変更シート
セキュリティ機能	ファイアウォール運用	□ 無効	□ 有効 □ 無効	□ 変更	ファイアウォール設定変更シート
	POP3・アンチウイルス運用	□ 無効	□ 有効 □ 無効	□ 変更	POP3設定変更シート
	メールアンチスパム運用	□ 無効	□ 有効 □ 無効	□ 変更	
	ファイル転送アプリ検出	□ 無効	□ 有効 □ 無効	□ 変更	IM/P2P設定変更シート
	メッセンジャーアプリ検出	□ 無効	□ 有効 □ 無効	□ 変更	IM/P2P設定変更シート

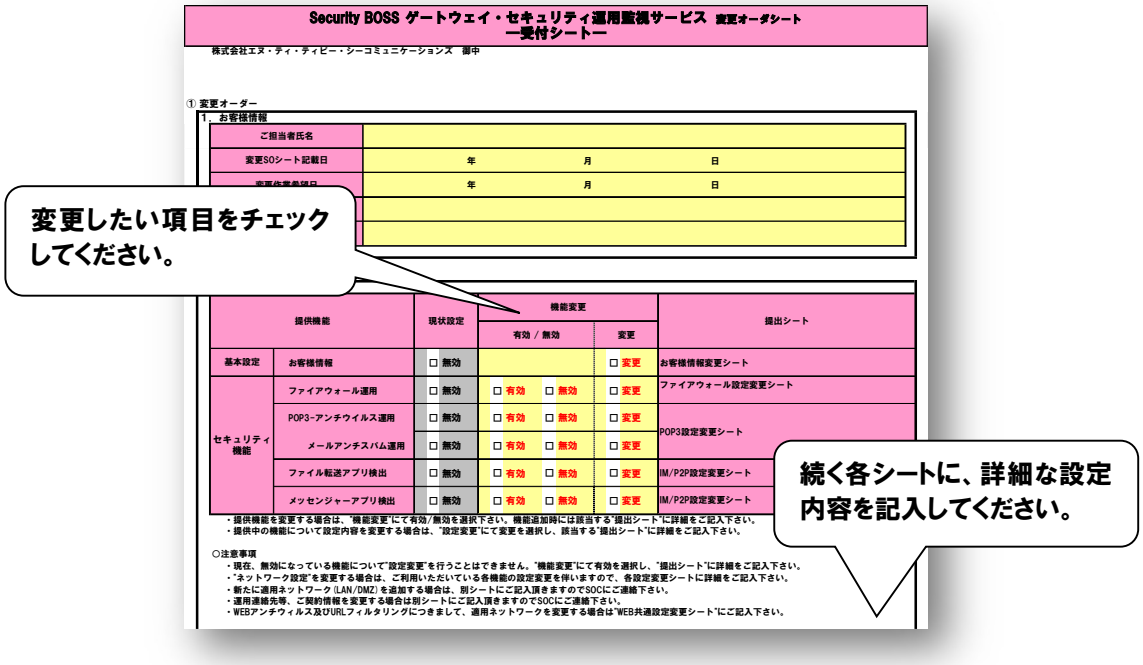
・提供機能を変更する場合は、"機能変更"にて有効/無効を選択下さい。機能追加時には該当する"提出シート"に詳細をご記入下さい。
・提供中の機能について設定内容を変更する場合は、"設定変更"にて変更を選択し、該当する"提出シート"に詳細をご記入下さい。

○注意事項
・現在、無効になっている機能について"設定変更"を行うことはできません。"機能変更"にて有効を選択し、"提出シート"に詳細をご記入下さい。
・"ネットワーク設定"を変更する場合は、ご利用いただいている各機能の設定変更を伴いますので、各設定変更シートに詳細をご記入下さい。
・新たに運用ネットワーク(LAN/DMZ)を追加する場合は、別シートにご記入頂きますのでSOCにご連絡下さい。
・運用連絡先等、ご契約情報を変更する場合は別シートにご記入頂きますのでSOCにご連絡下さい。
・WEBアンチウィルス及びURLフィルタリングにつきまして、運用ネットワークを変更する場合は"WEB共通設定変更シート"にご記入下さい。

図：5-4-2 変更オーダシート

［手順2］変更オーダシートへの記入

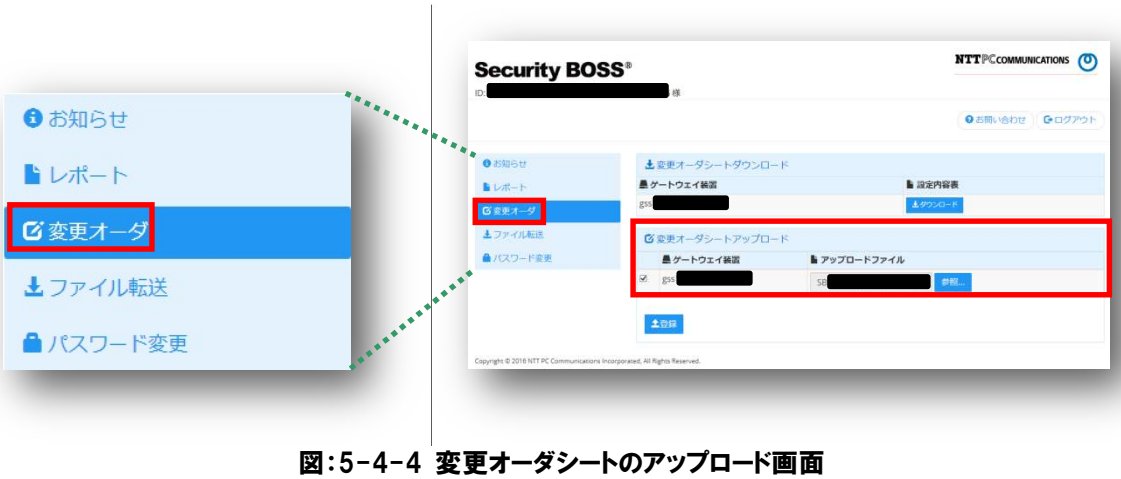
ダウンロードした『変更オーダシート』に、変更したい設定を記入してください。
記入が済んだら、お客さまの端末上にファイルを保存し、閉じてください。
※別のファイル名に変更して保存してもかまいません。



図：5-4-3 変更オーダシートの記入

［手順3］『変更オーダシート』アップロード画面の表示

お客さまの変更した『変更オーダシート』を、ユーザ・サポート・サイトへアップロードします。
画面左のメニューから『変更オーダ』を押下してください。



図：5-4-4 変更オーダシートのアップロード画面

［手順4］『変更オーダシート』のアップロード

①該当の『ゲートウェイ装置名』のチェックボックスに印をつけます。

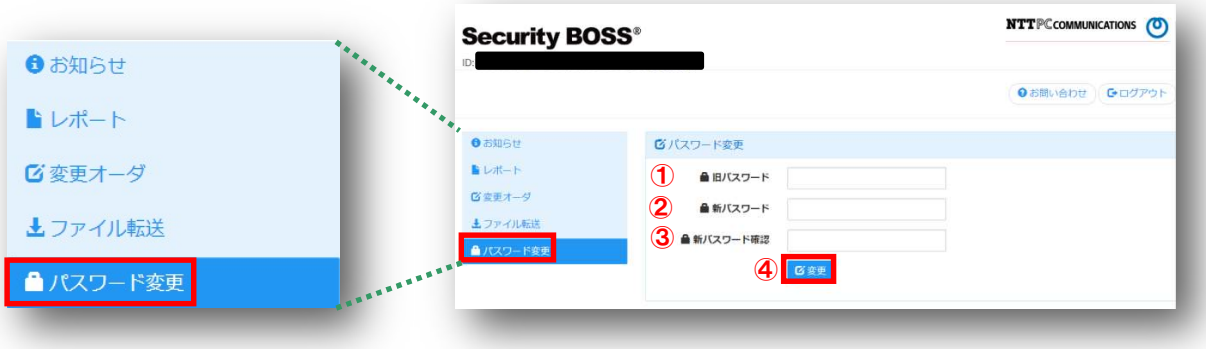
②『参照』を押下し、お客さまの新しく記入した『変更オーダシート』を選択します。

③ お客さまの新しく記入した『変更オーダシート』が表示されていることを確認し、『登録』を押下してください。
ユーザ・サポート・サイトを経由して、『変更オーダシート』がSOCへ送信されます。

図：5-4-5 変更オーダシートの送信

5－5 ログインパスワードの変更

［手順1］パスワード変更画面の表示
画面左のメニューから、『パスワード変更』を押下してください。
『パスワード変更』画面が表示されます。



図：5-5-1　パスワード変更画面の表示

［手順2］パスワード変更画面の表示
①『旧パスワード』に現在のパスワードを入力し、
②『新パスワード』と
③『新パスワード確認』に変更したいパスワードを入力してください。
④『変更』を押下してください。
お知らせ画面にて『パスワードを変更しました』と表示されれば完了です。

（注）半角英数記号で8文字以上32文字までのパスワードを設定してください。

（注）パスワードの書式詳細はパスワード変更画面を参照してください。

（注）3世代前までの使用済みパスワードは設定できません。

図：5-5-2　パスワード変更完了

ユーザ・サポート・サイトログインに使用するパスワード（セルフケアパスワード）は、定期的に変更をおこなってください。パスワードの登録から3ヶ月を経過しますと、ログイン時にパスワードの変更を促すメッセージが表示されます。

図：5-5-3 パスワード有効期限切れの表示

5回連続してログインに失敗した場合、アカウントが無効となり、ログインできなくなります。その際はSOCへ連絡し、パスワードの再発行を受けてください。

図：5-5-4 アカウントロックの表示

6. 不具合発生時の対処について

不具合が生じた場合には、以下の手順に従って対応をお願いいたします。

［手順１］不具合の内容の確認
① 現在発生している不具合の内容を確認してください。
② 不具合発生日時
③ 発生した状況（できるだけ詳細に）

［手順２］ゲートウェイ装置の確認
④ 電源ランプ（Power LED）が青く点灯していることを確認
⑤ イーサポートリンクランプが点灯していることを確認

［手順３］お客さま環境の確認
⑥ 不具合の発生したお客さま端末の特定
⑦ 不具合発生端末以外の端末で不具合が発生しているかの確認
⑧ 不具合の起きたアプリケーションの特定
例：Eメールが受け取れない → Eメールソフトの名前とバージョン
インターネットが閲覧できない → ブラウザの名前とバージョン
⑨ お客さまがご契約しているインターネットサービスプロバイダやアクセス回線事業に不具合が発生していないかの確認

［手順４］不具合についてのお問い合わせ
以上の確認をおこないましたらお電話、またはEメールにてSOCあてにご連絡ください。

～お電話の場合～
確認していただいた①～⑨の内容を踏まえて、ご説明いただきますようお願いいたします。

～Eメールの場合～
『７－１ お問い合わせ方法』を参照の上、件名にサービスIDと『不具合の問い合わせ』、本文に確認していただいた①～⑨の内容を記載し、SOCあてにお送りください。

ご連絡いただきましたお客さまには、当社にて確認・復旧作業をおこなった後、折り返しお電話・EメールによりSOCより結果をご連絡いたします。

６－１ 被疑機のお取り扱いについて

SOCがゲートウェイ装置本体の故障と判断した場合、被疑機の取り扱いについては、以下の流れとなります。

弊社からお客さまあてに代替機を発送いたします。代替機の交換が完了し、復旧確認が取れましたら、『７－１ お問い合わせ方法』を参照の上、お電話またはEメールにて代替機設置完了時刻をご連絡ください。その後、被疑機を弊社までお送りください。被疑機の送付先につきましては別途、SOCからご案内差し上げます。

６－２ 当社にて不具合を検知した場合

弊社がゲートウェイ装置の異常を検知した場合には、SOCにて確認・復旧作業をおこないます。復旧しない場合には、SOCよりお電話・Eメールにてご連絡いたします。

7. お問い合わせ

7－1 お問い合わせ方法

運用に関するお問い合わせは、Eメールやお電話にて受け付けております。Eメールの場合は、下記の例に従って件名にサービスIDとお問い合わせ内容を記載の上、SOCあてにご連絡ください。（Subject・本文のお客さま情報は、『Security BOSS サービス登録内容のご案内』に基づいて記載をお願いいたします。）

なお、回答は翌営業日以降となる場合がございます。あらかじめご了承ください。

件名	
サービス ID 依頼内容	gssxxx-xxxxx 『お問い合わせ内容』

本文	
お客さま情報	例
ご契約者名	㈱○○商事
お客さま番号	SBxxxxxxx
ご契約プラン	ライト・オンデマンド・ネクスト
ご担当者さま氏名	○○太郎
ご担当者さま E メールアドレス	taro@marumaru.co.jp
ご担当者さま 電話番号	03-1234-5678
お問い合わせ内容	

お問い合わせ先
NTTPC セキュリティ・オペレーション・センタ（SOC）
E－Mail: soc-all@nttpc.co.jp
0120-708-602（フリーダイヤル）

7－2 技術仕様についてのお問い合わせ

ゲートウェイ装置の技術仕様についてお問い合わせいただく際は、下記の例に従って、Eメールに
Subject・お客さま情報を記載の上、SOCあてにご連絡ください。（Subject・本文のお客さま情報は、『Security BOSSサービス登録内容のご案内』に基づいて記載をお願いいたします。）

なお、回答は翌営業日以降となる場合がございます。あらかじめご了承ください。

Subject	
サービスID	gssxxx-xxxxx 技術仕様に関する問い合わせ
依頼内容	

本文	
お客さま情報	例
ご契約者名	㈱○○商事
お客さま番号	SBxxxxxx
ご契約プラン	ライト・オンデマンド・ネクスト
ご担当者さま氏名	○○太郎
ご担当者さま Eメールアドレス	taro@marumaru.co.jp
ご担当者さま 電話番号	03-1234-5678
問い合わせ内容	

NTTPC技術サポート お問い合わせ先
E-Mail: soc-all@nttpc.co.jp

2023年4月