

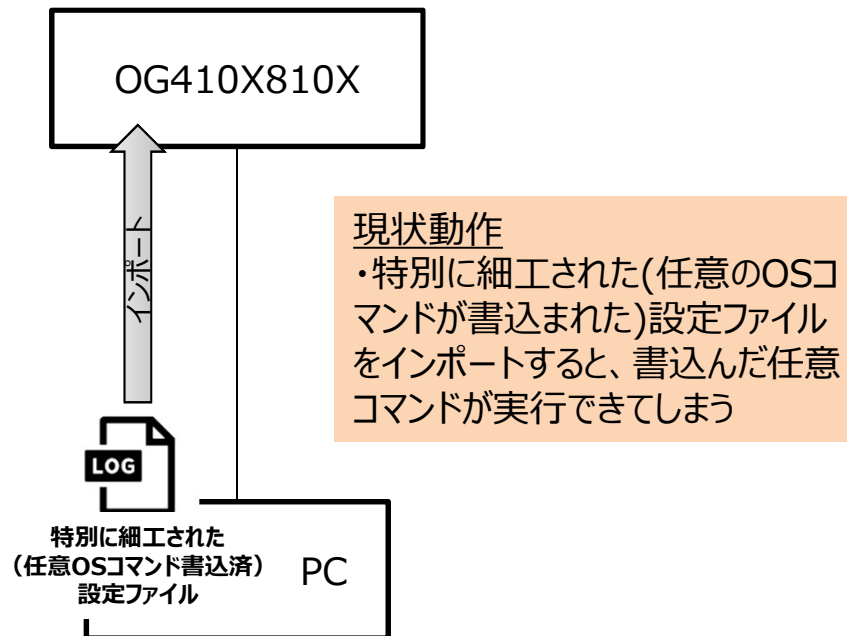
別紙 1_変更内容詳細 一覧

通番	項目	対象機種 (FW Ver.)	詳細内容 参照先
①	特別に細工された設定ファイルをインポートすることによりOSコマンドが実行できる脆弱性 (OSコマンドインジェクション) の対処	OG410X/810X (V2.32)	2ページ
②	工事保守者機能の改善		
	②-1.工事者アカウントの追加とパスワード初期値の変更		3ページ
	②-2.工事者用アカウント画面でのパスワード変更項目の追加		4ページ
	②-3.リモートメンテナンス設定での工事者用アカウントのログイン規制有無機能の追加		5ページ
	②-4.レポート表示機能「設定一覧表示」で表示される工事者用アカウントの追加		6ページ
	②-5.レポート表示機能「ログ表示/システムログ」で表示される工事者用アカウントの追加		7ページ
	②-6.telnet (ポート23) ポートの応答動作の改善		8ページ

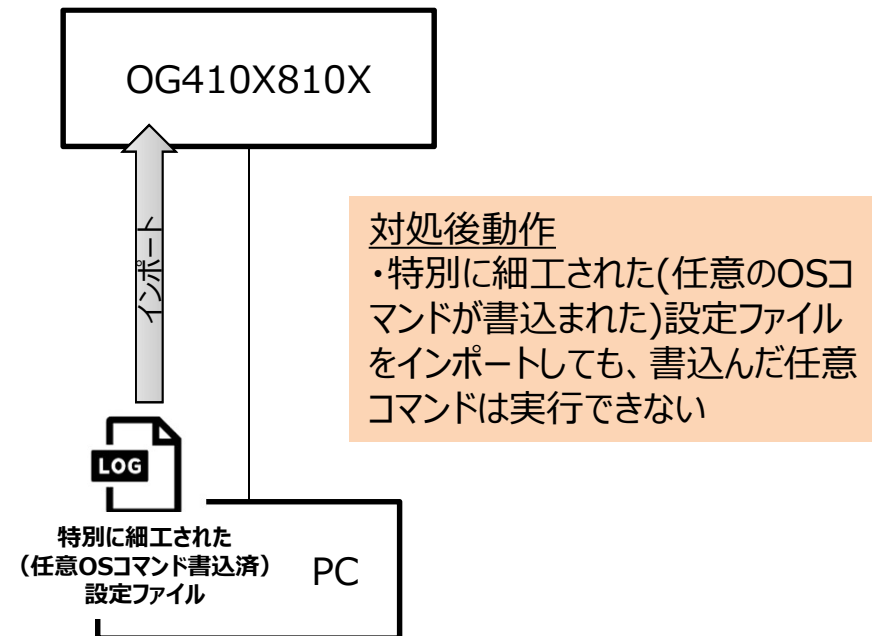
①. 特別に細工された設定ファイルをインポートすることによるOSコマンドが実行できる脆弱性（OSコマンドインジェクション）の対処

- 開発背景：エクスポート機能を用いてPC上に保存した設定ファイルに対し、特別な細工（任意のOSコマンドの書込み）を行いインポートすることで、書込んだ任意のOSコマンドを実行できてしまう脆弱性（OSコマンドインジェクション）の指摘を受けた。
- 開発内容：特別な細工（任意のOSコマンドの書込み）を行った設定ファイルをインポートしても、書込まれた任意のOSコマンドは実行できないように対処した。

現状の動作



対処後の動作



②-1.工事者アカウントの追加とパスワード初期値の変更

○開発背景：「①OSコマンドインジェクション」の指摘と合わせ工事保守マニュアルのみに記載している工事者アカウント情報が、インターネットのブログサイトに漏えいしていることの指摘を受けた。

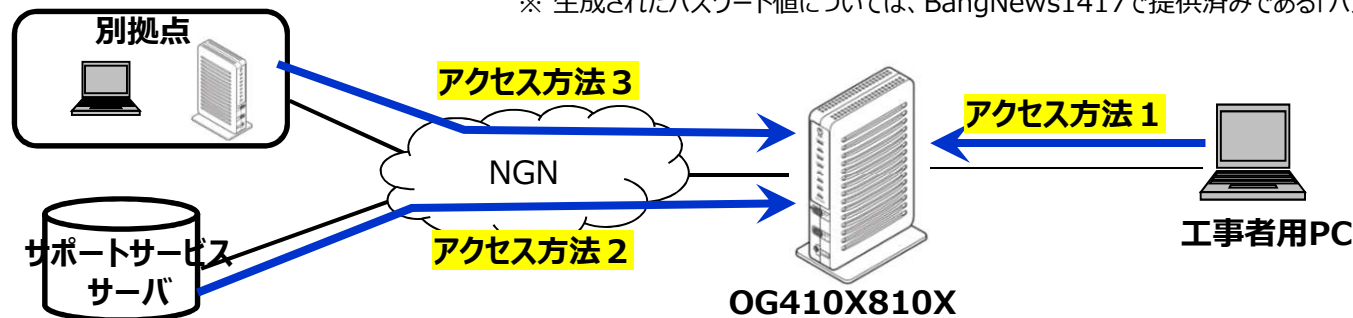
パスワードが悪意のある第3者に知れ渡った場合、電話番号等の機器情報が取得される等の恐れがあることから、パスワード初期値を機器個別のパスワードへ変更しセキュリティ強化を図る。

○開発内容：工事者アカウントのパスワード初期値を工事保守マニュアルに掲載のパスワードから、機器のWANポートのMACアドレスから生成された機器個別のパスワードに変更する。（下記図アクセス方法1）

あわせて、「サポートサービスサーバ経由でのアクセス」（下記図アクセス方法2）と「リモートメンテナンス機能を使ったアクセス」（下記図アクセス方法3）は遠隔拠点からのアクセスとなり、機器のMACアドレスが確認できないことから、新たに「サポートサービス用」と「リモートメンテナンス用」の工事者アカウントを追加する。

Web-GUIへのアクセス方法		現在の工事者用アカウント		Ver2.32～の工事者用アカウント	
		ID	パスワード (初期値)	ID	パスワード (初期値)
1	現地でのOGのLANからのアクセス (工事・故障対応)	Admin	工事保守マニュアルに記載しているパスワード	admin	WANのMACアドレスから生成されたパスワード※
2	サポートサービスサーバ経由でのアクセス（東のみ機能）			ossv-admin	工事保守マニュアルに記載しているパスワード
3	リモートメンテナンス機能を使ったアクセス			remote-admin	工事保守マニュアルに記載しているパスワード

※ 生成されたパスワード値については、BangNews1417で提供済みである「パスワード生成ツール」で確認ください。



②-2.工事者用アカウント画面でのパスワード変更項目の追加

- 開発背景：新たに「サポートサービス用」と「リモートメンテナンス用」の工事者アカウントを設けた際、パスワード初期値は設定されているが、セキュリティ強化の観点からパスワードは変更できるようにする。
- 開発内容：「サポートサービス用」と「リモートメンテナンス用」の工事者アカウントについて、パスワードを変更できるように「サポートサービス工事者用アカウント設定」画面と「リモートメンテナンス工事者用アカウント設定」画面をWeb-GUIに新たに設け、パスワードが変更できるようにする。

<Ver2.28での画面>

<Ver2.32で追加された画面>

メニュー追加

②-3.リモートメンテナンス設定での工事者用アカウントのログイン規制有無機能の追加

- 開発背景：リモートメンテナンス設定については、お客様が利用される際は基本ユーザアカウントを使用するが、セキュリティ強化としてお客様等による工事者アカウントでのアクセスを回避する。
- 開発内容：「リモートメンテナンス設定」画面内に、新たに「リモートからの工事者用アカウントでのWeb-GUIへのアクセス」の設定項目を追加し、リモートメンテナンス工事者アカウントでのアクセスに対して規制有無の切替設定を設ける。
 【設定値】・規制：リモートメンテナンス工事者用アカウントでのWeb-GUIへのログインを規制する（初期値）
 ・許可：リモートメンテナンス工事者用アカウントでのWeb-GUIへのログインを許可する

<Ver2.28での画面>

NTT
OG810Xa
ファームウェアバージョン 2.28

リモートメンテナンス設定

リモートメンテナンス機能 ☒ 有効 ☐ 無効

ホワイトリスト設定

※3～32桁の数字で入力してください。

接続先電話番号設定(発信側設定)

※3～32桁の数字で入力してください。

発信元電話番号設定(発信側設定)

※3～32桁の数字で入力してください。

接続状態 未接続

設定保存 接続 最新状態に更新

トップページへ戻る

<Ver2.32での画面>

NTT
OG810Xa
ファームウェアバージョン 2.32

リモートメンテナンス設定

リモートメンテナンス機能 ☒ 有効 ☐ 無効

ホワイトリスト設定

※3～32桁の数字で入力してください。

接続先電話番号設定(発信側設定)

※3～32桁の数字で入力してください。

発信元電話番号設定(発信側設定)

※3～32桁の数字で入力してください。

リモートからの工事者用アカウントでのWeb-GUIへのアクセス ☒ 規制 ☐ 許可

接続状態 未接続

設定保存 接続 最新状態に更新

トップページへ戻る

●規制(初期値)
→リモートメンテナンス工事者用アカウントでのWeb-GUIへのログインを規制する

●許可
→リモートメンテナンス工事者用アカウントでのWeb-GUIへのログインを許可する

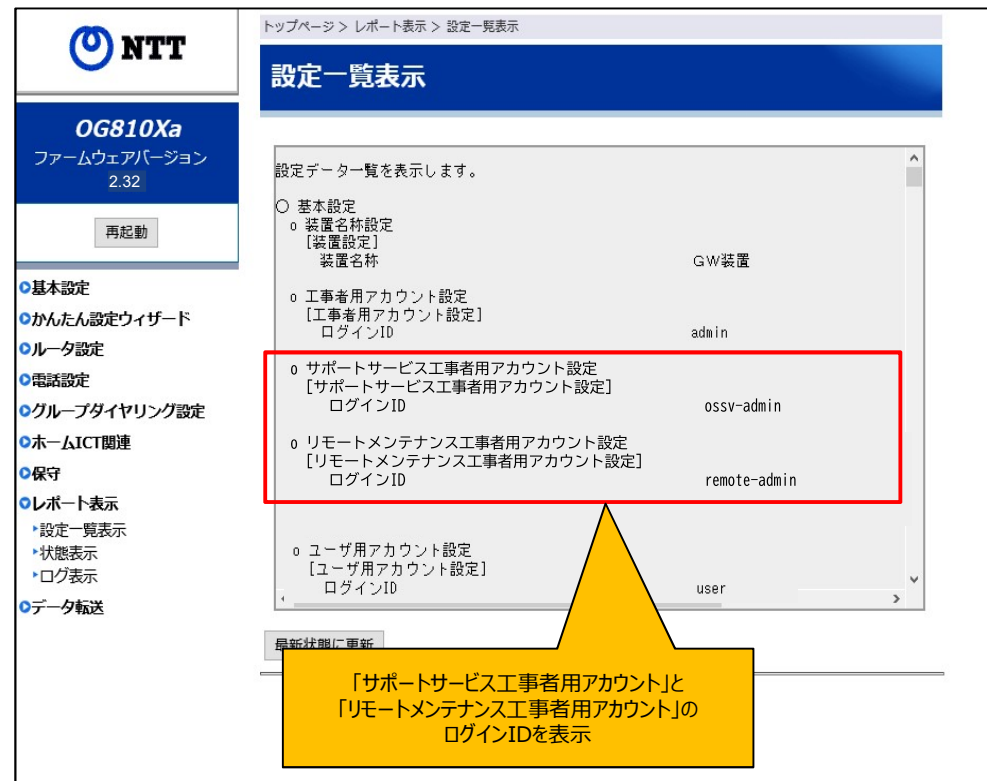
②-4.レポート表示機能「設定一覧表示」で表示される工事者用アカウントの追加

- 開発背景：「サポートサービス工事者アカウント」と「リモートメンテナンス工事者アカウント」の追加にともない、レポート表示機能内の「設定一覧表示」機能について、表示される内容を追加する。
- 開発内容：設定一覧表示画面にて、設定データ一覧を表示時、「サポートサービス工事者用アカウント」と「リモートメンテナンス工事者用アカウント」のログインIDを表示させる。

<Ver2.28での画面>



<Ver2.32での画面>



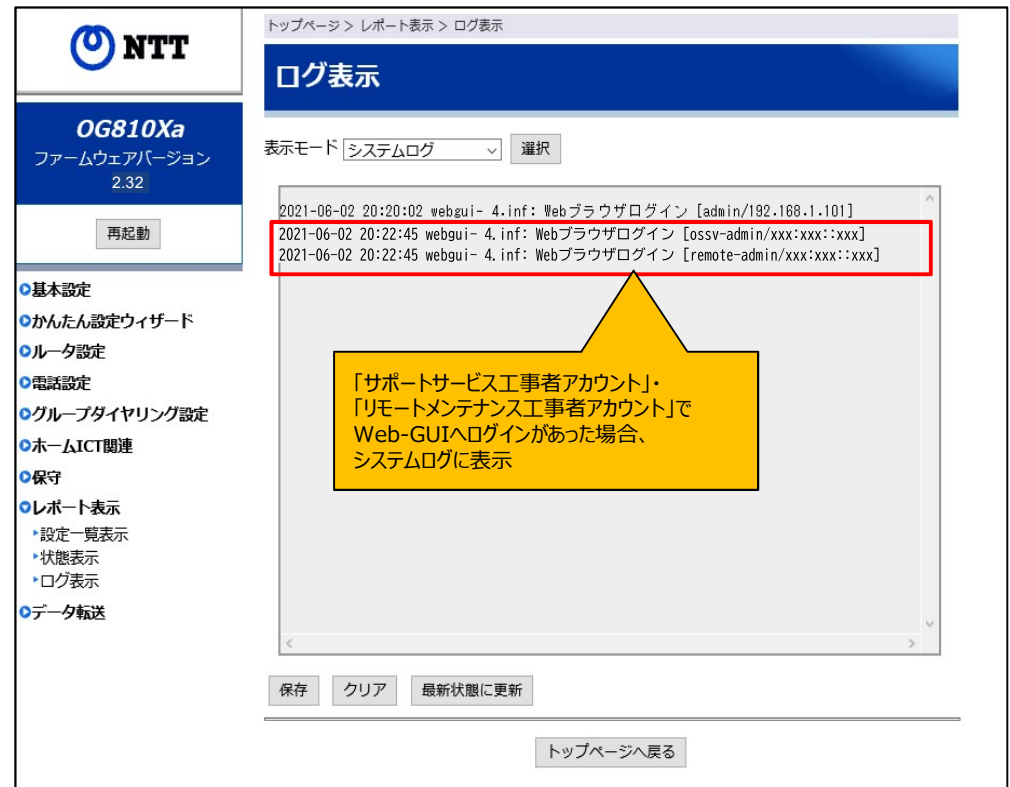
②-5.レポート表示機能「ログ表示/システムログ」で表示される工事者用アカウントの追加

- 開発背景：「サポートサービス工事者アカウント」と「リモートメンテナンス工事者アカウント」の追加にともない、レポート表示機能内の「ログ表示」機能について、表示される内容を追加する。
- 開発内容：「サポートサービス工事者アカウント」と「リモートメンテナンス工事者アカウント」でWeb-GUIへログインがあった場合、工事者アカウントと同様にシステムログ内に「ログイン日時」「IPアドレス」等の情報をシステムログに表示させる。

<Ver2.28での画面>



<Ver2.32での画面>



②-6.telnet（ポート23）ポートの応答動作の改善

- 開発背景：telnet(ポート23)ポートについては、LAN側からのアクセス時「ACKを応答」する仕様となっているが、セキュリティ強化の観点からから応答動作を変更する。
- 開発内容：LAN側からのtelnet(ポート23)ポートへのアクセス時の応答を、「ACKを応答」から「RSTを応答（未使用ポートへのアクセス）」へ変更する。

<Ver2.28でのtelnetポートの応答動作>

	アクセス元		
	LAN側	WAN側	
		ステルスモード有効時	ステルスモード無効時
応答動作	ACKを応答	無応答	無応答

<Ver2.32でのtelnetポートの応答動作>

	アクセス元		
	LAN側	WAN側	
		ステルスモード有効時	ステルスモード無効時
応答動作	RSTを応答	無応答	無応答