SITEGUARD

Proxy Edition
管理者用ガイド

― ウェブアプリケーションへの攻撃を水際で防ぐ
ウェブアプリケーション・ファイアウォール・ソリューション ―

Sample

EG Secure Solutions

1. SiteGuardについて

本製品は、オンラインショッピング、イントラネット、電子商取引、電子申請、情報検索、企業・官公庁での情報提供、個人間の情報交換等で利用されているウェブサーバー、ウェブアプリケーションへの攻撃を防ぐための「ウェブアプリケーション・ファイアウォール・ソリューション」です。

ウェブサーバー、ウェブアプリケーションへの攻撃は、情報漏えい・ウェブページやデータの改ざん等に繋がる重大な脅威です。特に、最近の電子商取引の普及、官公庁の電子化、各種 ASP サービス等によるウェブアプリケーションの普及と、世界的なインターネットの利用者増大により、攻撃が広がっています。企業の場合、個人情報漏洩・データ改ざん等の被害に加え、評判や信頼の低下による間接的な影響もあります。

システム管理者は本製品を使用することで、ウェブアプリケーションとの通信の監視を一箇所で集中的に行うことができます。
本製品は、ソフトウェア製品(HTTP プロキシ)のため、ウェブサーバーと同一環境にインストールして利用することも可能です。

防御機能には、シグネチャ検査、パラメータ検査、Cookie 暗号化、セッション管理、応答ヘッダフィールド追加・削除等があり、以下のような各種攻撃に対応しています。

- SQL インジェクション
- クロスサイトスクリプティング(XSS)
- クロスサイトリクエストフォージェリ(CSRF)
- ディレクトリトラバーサル
- OS コマンドインジェクション
- HTTP ヘッダインジェクション
- フォースブラウジング
- ブルートフォース
- クリックジャッキング

また、完全な国産製品となっているため、管理画面の言語やドキュメント類の提供などはすべて日本語対応となっています。

4. インストール

本製品は、rpm パッケージ、または tar.gz パッケージによるインストールが可能です。

- 通常は、rpm パッケージを使用します。
- インストールのオプションを指定する場合、tar.gz パッケージを使用します。
- インストール先のディレクトリは、/opt/jp-secure/siteguard(デフォルト)です。

インストールパッケージは、32bit 用と 64bit 用があります。
ご利用の環境に合ったインストールパッケージを使用してください。

■rpm パッケージ

- siteguard-proxy-edition-*XXX-X*.**i386**.rpm **32bit 版**
- siteguard-proxy-edition-*XXX-X*.**x86_64**.rpm **64bit 版**

■tar.gz パッケージ

- siteguard-proxy-edition-*XXX-X*.**i386**.tar.gz **32bit 版**
- siteguard-proxy-edition-*XXX-X*.**x86_64**.tar.gz **64bit 版**

本製品のインストールにより、以下のディレクトリが作成されます。

ディレクトリ名	説明
/opt/jp-secure/siteguard/	インストールディレクトリ(デフォルト)
/opt/jp-secure/siteguard/conf/	ウェブ管理画面、ライセンス等の全体設定
/opt/jp-secure/siteguard/log/	ウェブ管理画面、シグネチャ更新ログ
/opt/jp-secure/siteguard/statistics/	統計データ
/opt/jp-secure/siteguard/reports/	レポートファイル
/opt/jp-secure/siteguard/proxy/*XX*	各インスタンス毎のディレクトリ
/opt/jp-secure/siteguard/proxy/*XX*/conf/	各インスタンス毎の設定
/opt/jp-secure/siteguard/proxy/*XX*/log/	各インスタンス毎のログ
/opt/jp-secure/siteguard/proxy/XX/statistics/	各インスタンス毎の統計データ

XX:インスタンス番号

4.1 インストール（rpm パッケージ）

rpm パッケージを使用して、本製品をインストールする方法について説明します。

root 権限で、以下のコマンドを実行します。

```
# rpm -Uvh siteguard-proxy-edition-XXX-X.x86_64.rpm
```

インストール完了のメッセージを確認します。

```
------------------------------------------------
 Install succeeded!
 Please access following URL for starting proxy
 http://hostname:9014/
 (default user:admin, default password:admin)
------------------------------------------------
```

以上でインストールが完了し、ウェブ管理画面が利用できるようになります。
続いて「5. 初期設定」を参照してください。

4.2 インストール（tar.gz パッケージ）

本製品は、tar.gz パッケージを使用したインストールも可能です。
インストールオプションを指定する場合は、「4.3 インストールコマンドの詳細な利用方法」を参照してください。

root 権限で、以下のコマンドを実行します。

```
# tar -zxvf siteguard-proxy-edition-XXX-X.x86_64.tar.gz
# cd siteguard-proxy-edition-XXX/
# make install
```

インストール完了のメッセージを確認します。

```
------------------------------------------------
 Install succeeded!
 Please access following URL for starting proxy
 http://hostname:9014/
 (default user:admin, default password:admin)
------------------------------------------------
```

以上でインストールが完了し、ウェブ管理画面が利用できるようになります。
続いて「5. 初期設定」を参照してください。

5.1.3 ホーム画面

検出情報の統計グラフのほか、各プロキシの設定情報のサマリを確認することができます。
マルチインスタンスの管理もホーム画面から行います。

アイコン	説　明
	該当のプロキシのサービスが起動中であることを示しています。
	該当のプロキシのサービスが停止中であることを示しています。
	該当のプロキシの攻撃検査、各機能が”有効”であることを示しています。 有効にしている機能は、緑のチェックで表示されます。
	該当のプロキシの攻撃検査、各機能が”無効”であることを示しています。 無効にしている機能は、チェックなし(グレー)で表示されます。

➔ 統計グラフについては、「12.　統計・レポート」を参照してください。
➔ マルチインスタンスについては、「13.　マルチインスタンス」を参照してください。

5.2 ウェブ管理画面の構成

ウェブ管理画面は、画面上部のメニューと下部の操作エリアから構成されます。
以下の画面は、メインメニュー**[プロキシ設定]**→サブメニュー**[接続設定]**を選択したときの画面です。

項　目	説　明
トップメニュー メインメニュー サブメニュー	本製品の各種設定やログ閲覧を行うためのメニューです。 設定したい項目をクリックすると、操作エリアに選択した項目の設定ページが表示されます。
操作エリア	各項目を設定するエリアです。 デフォルト値が設定されていますので、必要に応じて変更してください。
サービス起動・停止・再起動ボタン	プロキシサービスの起動・停止・再起動を行うためのボタンです。
有効/無効ボタン 選択ボタン	各種機能の有効/無効の設定やモードの選択で使用します。
保存・再起動・キャンセルボタン	設定後、〔保存〕ボタンをクリックすると、設定した内容を保存し、〔保存・再起動〕ボタンをクリックすると、設定した内容を保存してサービスを再起動します。 〔キャンセル〕ボタンをクリックすると、保存されていない設定内容は破棄されます。

Note

各種機能の設定で〔保存・適用〕ボタンが配置されているページでは、〔保存・適用〕ボタンを押すことで設定内容の保存と適用ができます。

7. 詳細設定

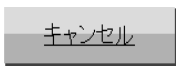
7.1 プロキシ設定

本製品のインストールと動作確認が完了したら、必要に応じて各種機能の詳細設定を行います。
設定するときは、メインメニューの〔プロキシ設定〕を選択します。

項目をサブメニューから選択し、設定を行います。

必要な設定を行い、画面上部のサービス起動・停止・再起動ボタン  または、画面下部の〔保存〕〔保存・再起動〕ボタンで設定内容の保存とサービスの起動を行います。

■アイコン/ボタンに関する説明

アイコン/ボタン	説　明
	サービスが停止中であることを示しています。
	サービスが起動中であることを示しています。
	設定の保存とサービスの起動を行います。 (サービス起動中は、グレー表示となり、押すことはできません。)
	設定の保存とサービスの停止を行います。 (サービス停止中は、グレー表示となり、押すことはできません。)
	設定の保存とサービスの再起動を行います。 (サービス停止中は、グレー表示となり、押すことはできません。)
	設定内容を保存します。
	設定内容を保存し、サービスを再起動します。
	保存されていない設定内容を破棄します。

Note

各設定項目の（　）は、設定ファイル（proxy/XX/conf/siteguard.ini）での項目名です。
ウェブ管理画面を使用せずに、設定ファイルを編集することも可能ですが、通常はウェブ管理画面を使用してください。

7.1.6 シグネチャ検査の詳細設定項目・設定例

シグネチャ検査には、本製品に実装されているトラステッド・シグネチャによる検査と、お客様自身でシグネチャを作成することができるカスタム・シグネチャによる検査があります。
カスタム・シグネチャでは、条件を指定した検出の除外設定を行うこともできます。

7.1.6.1 トラステッド・シグネチャの設定

トラステッド・シグネチャによる検査を行うことで、SQL インジェクションやクロスサイトスクリプティングなどの攻撃を防御することができます。
[**トラステッド・シグネチャの設定**]画面では、各シグネチャの有効・無効、検出時の動作を設定できます。シグネチャは、1 ページあたり、50 個の単位で表示されます。

■ボタンに関する説明

アイコン/ボタン	説　明
置換	シグネチャの有効/無効、動作を置換します。
リセット	シグネチャの設定を既定値（推奨シグネチャ設定）にリセットします。
検索	検索文字列に入力したシグネチャを検索します。 シグネチャ ID または、シグネチャ名の前方一致で検索します。
保存	編集した設定内容を保存します。
保存・適用	編集した設定内容の保存と適用を行います。
閉じる	トラステッド・シグネチャの設定画面を閉じます。

〔置換〕ボタンと〔リセット〕ボタンが適用される範囲は、表示されているページ数の範囲となります。以下の表示では、11 ページ分のシグネチャが適用範囲となります。

シグネチャ名(例.sqlinj)で検索すると、該当するシグネチャだけが抽出され、ページ数の表示は以下のようになります。(前方一致)

この場合、3 ページ分のシグネチャが〔置換〕ボタンと〔リセット〕ボタンの適用範囲となります。

Note

すべてのシグネチャを対象に”無効”に置換したあと、SQL インジェクション対策用のシグネチャを検索し、”有効”に置換するといった操作が可能です。
(SQL インジェクション対策のみのシグネチャ設定を作成する場合の例)

8. コマンドラインでの操作

本章では、シグネチャの更新やサービスの起動・停止などをコマンドラインで実行する場合の操作方法を説明しています。

通常、コマンドラインでの操作は必要ありません。

8.1 製品バージョン確認コマンド

■動作概要

インストールされている製品のバージョン情報を表示します。

■コマンド名

```
cd /opt/jp-secure/siteguard; make show_webui_version
```

■コマンド例

製品のバージョン情報を表示します。

```
# cd /opt/jp-secure/siteguard; make show_webui_version
```

8.2 設定情報適用コマンド

■動作概要

変更・保存した設定情報を適用します。ウェブ管理画面の〔保存・適用〕ボタンと同じ動作です。

■コマンド名

```
cd /opt/jp-secure/siteguard; make instance_no=XX reconfig
```

■コマンド例

指定したインスタンス(XX:インスタンス番号)の設定情報を適用します。

※2 番目のインスタンスを指定した場合の例

```
# cd /opt/jp-secure/siteguard; make instance_no=2 reconfig
```

全インスタンスの設定情報を適用します。

```
# cd /opt/jp-secure/siteguard; make reconfig
```

make reconfig によって、設定の適用ができるのは、ウェブ管理画面で〔保存・適用〕ボタンがある設定項目です。

8.3 シグネチャ更新コマンド

■動作概要

シグネチャファイル(トラステッド・シグネチャ)を最新版に更新します。
ウェブ管理画面の**[手動更新]**および**[自動更新]**で実行されるコマンドです。
シグネチャ更新時の設定は、「7.2　シグネチャ更新設定」の内容にしたがいます。

シグネチャ更新コマンド(dbupdate_waf)の処理

wget で、https://www.jp-secure.com/download/siteguard/updates_waf4/latest-waf.zip に接続し、シグネチャファイル(latest-waf.zip)を updates_waf ディレクトリにダウンロードします。
次に、latest-waf.zip を展開し、更新が必要な場合は、シグネチャファイルを databases_waf ディレクトリにコピーします。最後に、設定をマージして、proxy/*XX*/conf/waf ディレクトリのシグネチャファイルを更新します。
シグネチャバージョンは、databases_waf/header.ini の"[WAF_Database_Version]"の値を参照します。(Version=YYYY-MM-DD_XX)

■コマンド名

/opt/jp-secure/siteguard/dbupdate_waf

■オプション

-v　更新結果を、ログファイル以外（標準出力および標準エラー出力）に表示します。

■コマンド例

シグネチャファイルを更新します。

```
# cd /opt/jp-secure/siteguard; ./dbupdate_waf
```

シグネチャファイルを更新し、更新状況を syslog に出力します。

```
# cd /opt/jp-secure/siteguard; ./dbupdate_waf -v 2>&1| logger -t dbupdate_waf -p local0.err
```

本製品を導入したサーバーからインターネットへの接続が行えない場合、インターネット接続が可能な管理用 PC などを利用してシグネチャを更新することができます。

管理用 PC などからサポートページにログインして、最新のシグネチャファイル(latest-waf.zip)を取得します。
その後、本製品を導入したサーバーの任意のディレクトリにシグネチャファイルを配置して、以下のように dbupdate_waf コマンドを実行します。

例）/var/tmp に latest-waf.zip を配置した場合
 # cd /opt/jp-secure/siteguard;./dbupdate_waf /var/tmp/latest-waf.zip

■終了コード

更新成功時は 0 を、失敗時は 0 以外を返します。

■ログファイル

更新結果は、以下のログファイルに記録されます。

/opt/jp-secure/siteguard/log/dbupdate_waf.log　シグネチャ更新結果の履歴
/opt/jp-secure/siteguard/log/dbupdate_waf_last_result.txt　wget の実行結果

11. 設置・構成例

本章では、ロードバランサを用いた負荷分散環境や HTTPS(SSL)を検査する場合などの設置・構成例について説明します。

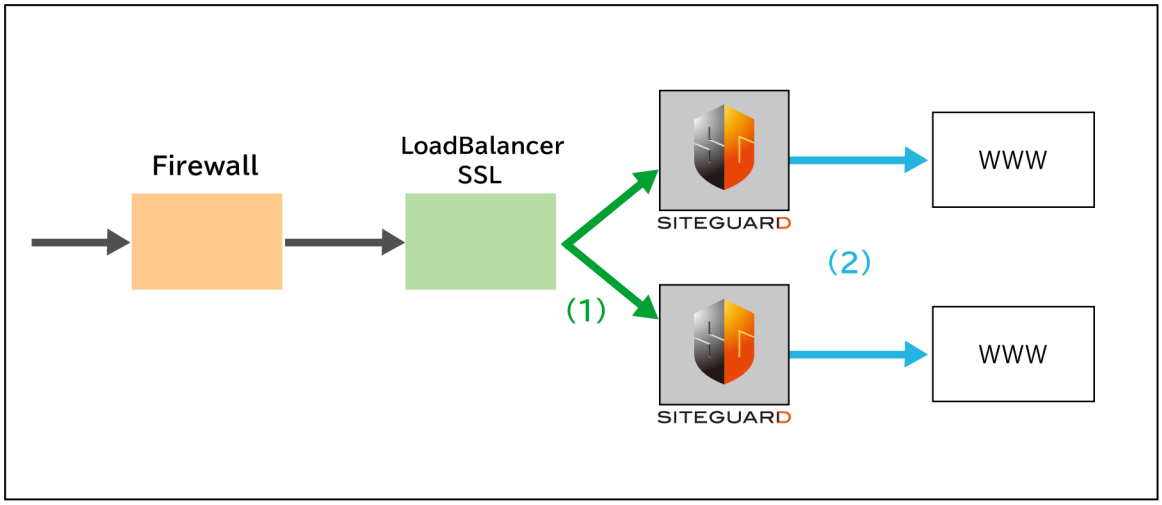
本製品は、HTTP のプロキシとして動作します。
HTTPS(SSL)の検査を行う場合は、本製品の前段に SSL プロキシや SSL アクセラレータ等を設置し、本製品が HTTP で検査できる構成にしてください。

11.1 負荷分散・冗長構成

ロードバランサを用いた環境で、本製品を使用する場合の構成例です。

11.1.1 負荷分散・冗長構成の接続イメージと設定例

■構成例①



(1) ロードバランサがインターネット側から受信したリクエストを SiteGuard に振り分けます。
(SiteGuard は、HTTP プロキシとして動作するため、HTTPS(SSL)はロードバランサで終端します。)
(2) SiteGuard は、検査済みのリクエストを中継します。
ここでは、SiteGuard とウェブサーバ(WWW)が 1 対 1 の構成となっています。

■設定例

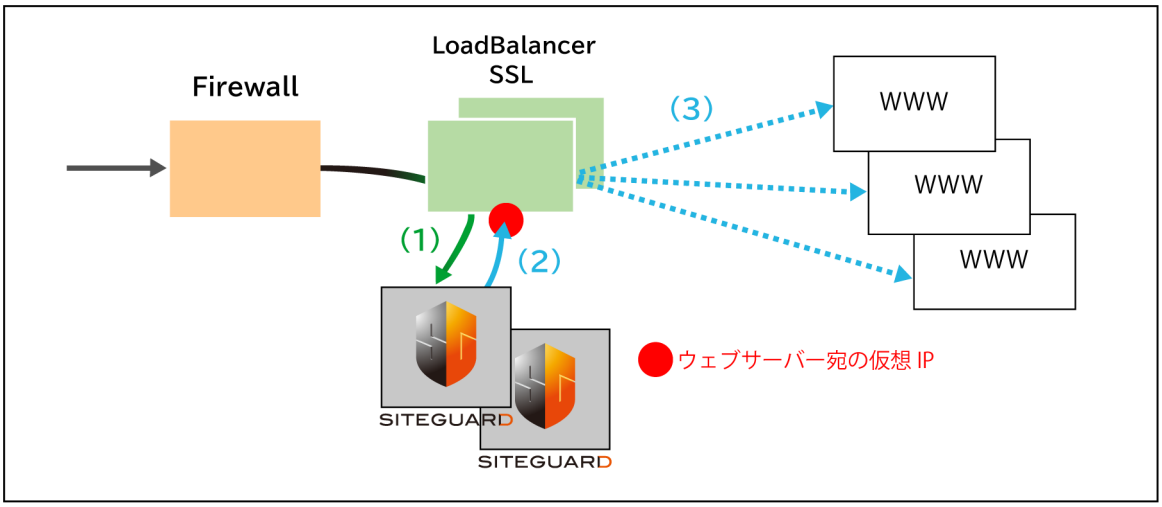
ウェブ管理画面で、SiteGuard の待ち受けポート番号と、親サーバを設定します。

［接続設定］
［ポート番号］：　SiteGuard の待ち受けポート番号
［接続モード］
［親サーバ］：　選択
［ホスト名］：　WWW の IP アドレス
［ポート番号］：　WWW のポート番号

設定後、〔起動〕ボタン  または、〔再起動〕ボタン  を押すことで、設定内容が保存され、サービスが起動(再起動)します。

構成例では、2 台の SiteGuard を設置しています。それぞれの SiteGuard で同様の設定を行ってください。

■構成例②



(1) ロードバランサがインターネット側から受信したリクエストを SiteGuard に振り分けます。
(SiteGuard は、HTTP プロキシとして動作するため、HTTPS(SSL)はロードバランサで終端します。)
(2) SiteGuard は、検査済みのリクエストを中継します。
ここでは、ロードバランサに設定されているウェブサーバー宛の仮想 IP 宛に中継しています。
(3) SiteGuard によって中継されたリクエストをロードバランサがウェブサーバーに振り分けます。

■設定例

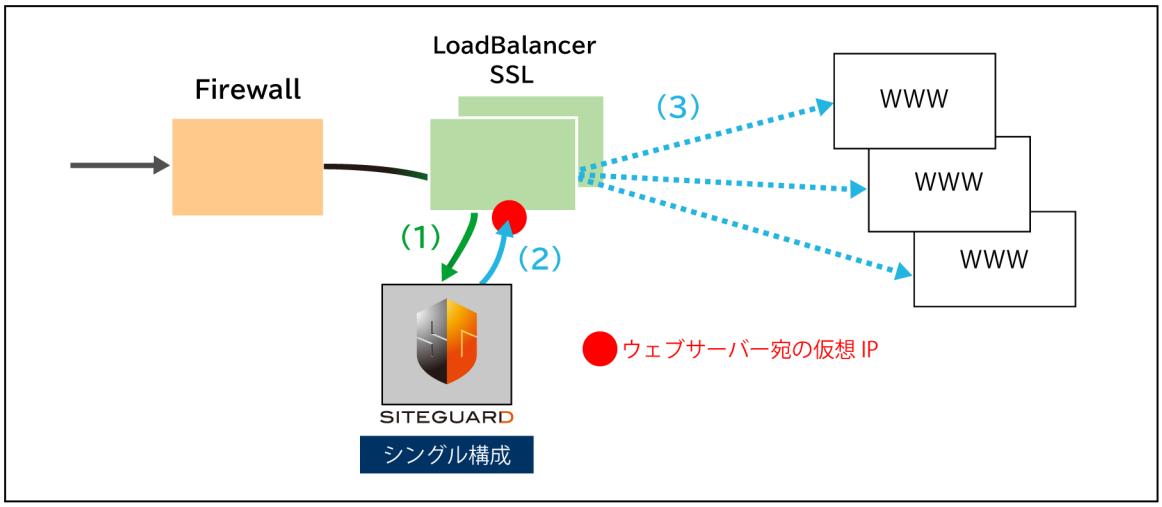
ウェブ管理画面で、SiteGuard の待ち受けポート番号と、親サーバを設定します。

［接続設定］
［ポート番号］：　SiteGuard の待ち受けポート番号
［接続モード］
［親サーバ］：　選択
［ホスト名］：　ロードバランサの IP アドレス(ウェブサーバー宛の仮想 IP)
［ポート番号］：　ロードバランサのポート番号

設定後、〔起動〕ボタン  または、〔再起動〕ボタン  を押すことで、設定内容が保存され、サービスが起動(再起動)します。

構成例では、2 台の SiteGuard を設置しています。それぞれの SiteGuard で同様の設定を行ってください。

■構成例③



(1) ロードバランサがインターネット側から受信したリクエストを SiteGuard に振り分けます。
(SiteGuard は、HTTP プロキシとして動作するため、HTTPS(SSL)はロードバランサで終端します。)
(2) SiteGuard は、検査済みのリクエストを中継します。
ここでは、ロードバランサに設定されているウェブサーバー宛の仮想 IP 宛に中継しています。
(3) SiteGuard によって中継されたリクエストをロードバランサがウェブサーバーに振り分けます。

■設定例

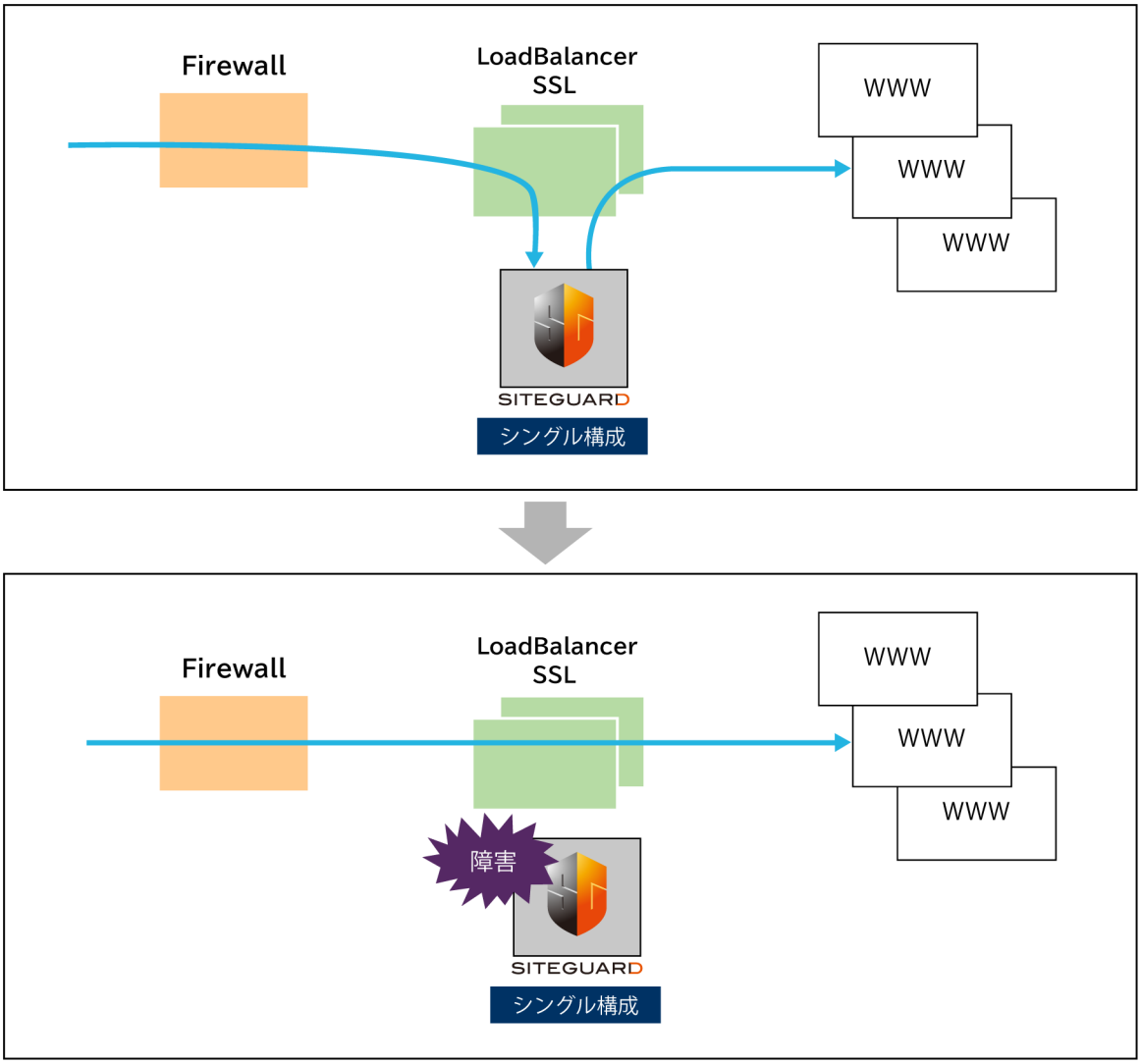
ウェブ管理画面で、SiteGuard の待ち受けポート番号と、親サーバを設定します。

［接続設定］
［ポート番号］：　SiteGuard の待ち受けポート番号
［接続モード］
［親サーバ］：　選択
［ホスト名］：　ロードバランサの IP アドレス(ウェブサーバー宛の仮想 IP)
［ポート番号］：　ロードバランサのポート番号

設定後、〔起動〕ボタン  または、〔再起動〕ボタン  を押すことで、設定内容が保存され、サービスが起動(再起動)します。

Note

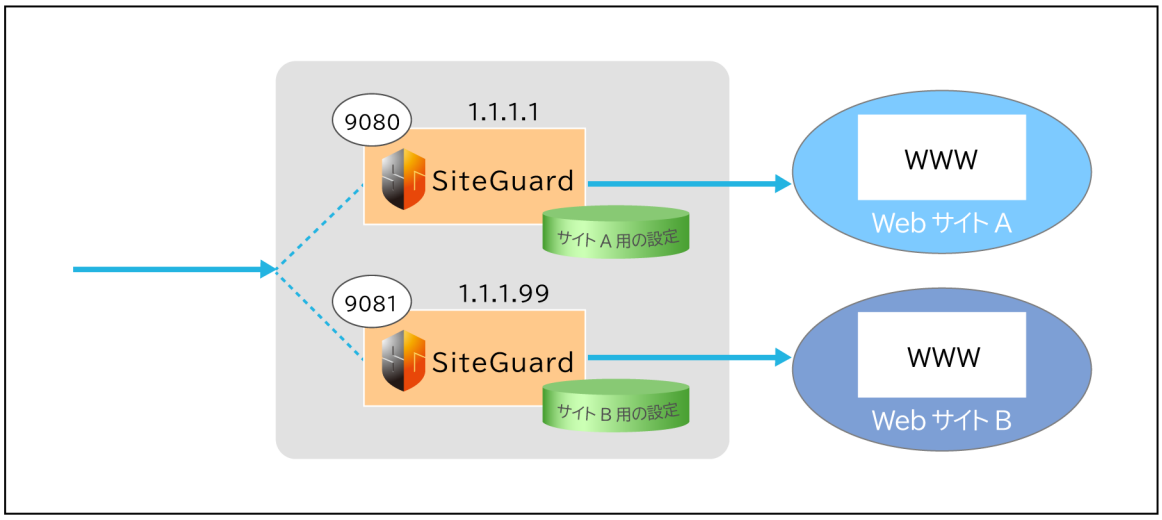
構成例③は、シングル構成となっています。
本製品の障害検知時は、ロードバランサ側で以下のように通信経路を切り替えることで、サービスの継続が可能です。



13. マルチインスタンス

13.1 マルチインスタンスの設定

本製品は、異なる設定を持つプロキシ(インスタンス)を最大 20 個まで起動することができます。
サイトごとに本製品の設定を変えたり、本運用とテスト用の設定を用意するといった対応が可能です。



13.1.1 プロキシの追加と複製

〔プロキシを追加〕ボタンを押すと、デフォルト設定のプロキシが追加されます。
〔複製〕ボタンを押すと、該当のプロキシの設定を複製し、新たにプロキシを追加します。
いずれも停止の状態でプロキシが追加されますので、必要に応じて、各種設定変更を行い、サービスを起動してください。
各種設定は、各プロキシごとに行うことができます。

13.1.2 プロキシの削除

〔削除〕ボタンを押すと、該当のプロキシが削除されます。
〔削除〕ボタンは、停止しているプロキシに対してのみ表示されます。
また、No.01 のプロキシに〔削除〕ボタンはありません。

■アイコン/ボタンに関する説明

アイコン	説　明
	該当のプロキシのサービスが起動中であることを示しています。
	該当のプロキシのサービスが停止中であることを示しています。
	該当のプロキシの攻撃検査、各機能が”有効”であることを示しています。 有効にしている機能は、緑のチェックで表示されます。
	該当のプロキシの攻撃検査、各機能が”無効”であることを示しています。 無効にしている機能は、チェックなし(グレー)で表示されます。
	デフォルトの設定でプロキシを追加します。
	該当のプロキシの設定を複製し、新たにプロキシを追加します。
	該当のプロキシを削除します。