"はかる"技術で未来を創る
東陽テクニカ

spirent

アプリケーション&セキュリティ・テストソリューション

cyberflood avalanche

CF400

C100-S3-MP

C200

CF30

INDEX

CyberFlood　Avalanche

CyberFlood/ Avalancheは米国Spirent Communications社が提供するL4-7のテスターです。アプリケーションレイヤのトラフィックを擬似し、スループット、CPS（コネクション/秒）、TCP同時接続数試験やセキュリティ試験としてご活用いただけます。
それぞれの用途に合わせて、1つのプラットフォームでモードを切り替えることでご利用いただけます。

CyberFlood

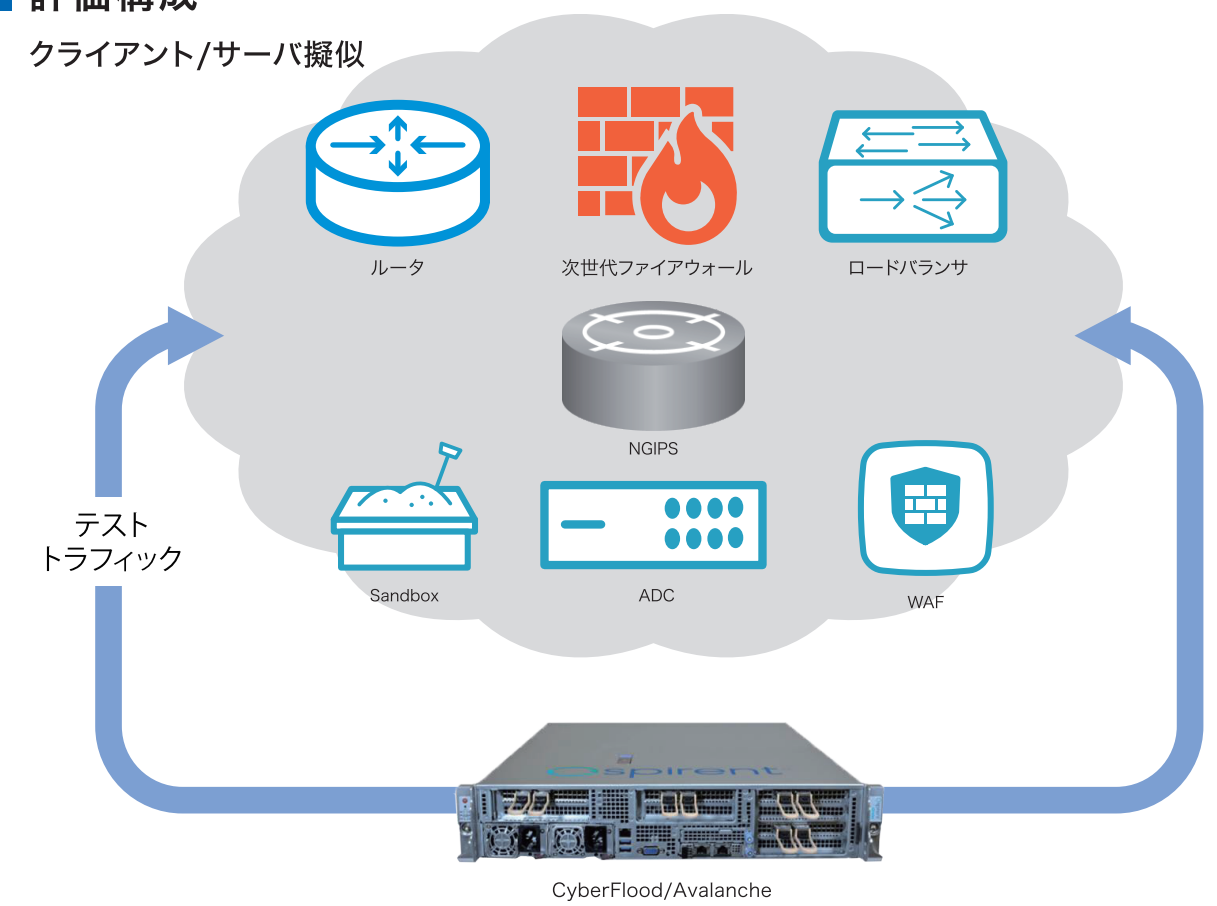
CyberFloodは、ファイアウォールやIPSなどのNW機器に対し、セキュリティ試験、アプリケーション試験、パフォーマンス試験が可能です。マルウェアや脆弱性を突く攻撃トラフィックを流すことで遮断の可否を試験でき、様々なアプリケーションミックストラフィックによるパフォーマンス測定も可能です。シンプルなインタフェースで簡単に試験の設定ができ、Rest APIで試験の自動化も可能です。

Avalanche

Avalancheは、ハイパフォーマンスかつリアルなトラフィック生成ができ、様々なプロトコルをサポートし、お客様の環境に合わせた細かな設定が可能です。ファイアウォールやロードバランサを含めたシステム試験、プロキシや実サーバへの負荷試験も可能です。

評価構成

クライアント/サーバ擬似



クライアント擬似

CyberFlood とは

https://www.toyo.co.jp/ict/products/detail/cyberflood.html

TestCloudシナリオベースでリアルな試験トラフィックを使い、パフォーマンス試験やセキュリティ試験を簡単に行うことができます。

主な試験

-パフォーマンス試験
-ミックストラフィック試験
-セキュリティ試験

リアルなシナリオを定期更新
アプリケーション：23,000以上
既知の脆弱性：5,300以上
マルウェア：81,000以上
（2021年11月現在）

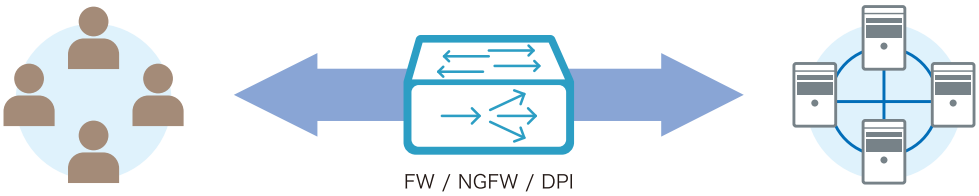
ブラウザベースのGUIから簡単設定！

シナリオ選択　簡単試験設定　試験中モニタ　結果レポート

パフォーマンス測定機能

試験構成や印加トラフィックの値を設定することで、簡単にパフォーマンスの測定をすることができます。
HTTP/HTTPSスループット試験、DNS試験が実施可能です。

□構成例



□試験例（HTTPS試験の場合）

SSL/TLS設定　設定した負荷量と実際の負荷量の比較　結果レポート：合格/不合格表示

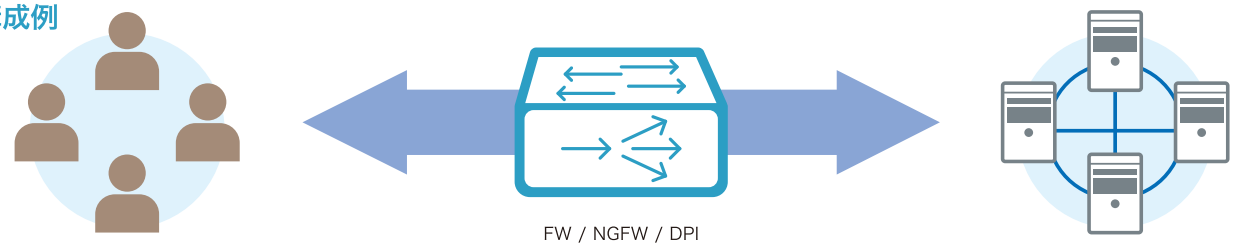
ミックス トラフィック試験

様々なプロトコルや、20,000種類以上のリアルなアプリケーション擬似トラフィックを混在させた環境でのスループット試験の測定が可能です。
アプリケーションごとに制御を行う次世代ファイアウォールやDPI装置などが各種アプリケーショントラフィックを想定通りに制御できているかを評価することが可能です。

■アプリケーションシナリオはSpirent TestCloudにより定期的に更新
■実環境に合わせて自由にアプリケーションを混在させたカスタムミックス試験に加えて、攻撃トラフィック混在可能
■アプリケーションごとのパフォーマンス結果および攻撃トラフィックの検知可否や検知率が取得可能
■Smart Apps（新シナリオ・パッケージ）
従来のシナリオパッケージに加え、テレワーク通信を意識したコンテンツ（Office365、Zoom、Netflix等）がテストクラウドコンテンツに含まれています。よりリアルなトラフィックを使った負荷試験が可能です。


アプリケーションシナリオ例

□構成例



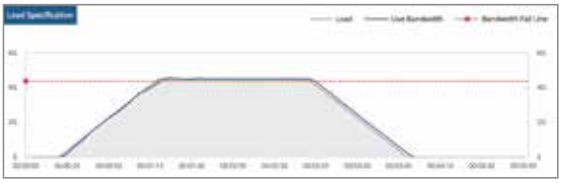
クライアント
（CyberFlood）

サーバ
（CyberFlood）

□試験例

正常系トラフィックのみの試験の場合

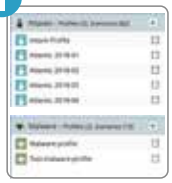

様々なアプリケーション
ミックスした設定

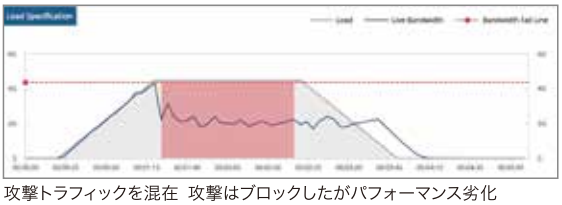

正常なトラフィック

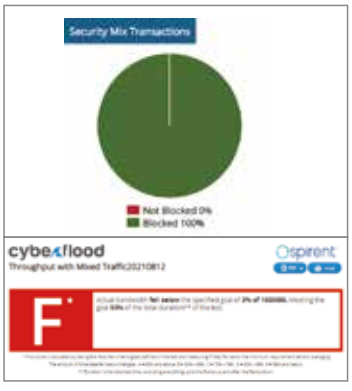
結果レポート：
設定した閾値を満たす結果で合格判定

異常系トラフィックを混入させた試験の場合


アプリケーション
ミックスに
攻撃トラフィックを追加




攻撃トラフィックを混在 攻撃はブロックしたがパフォーマンス劣化



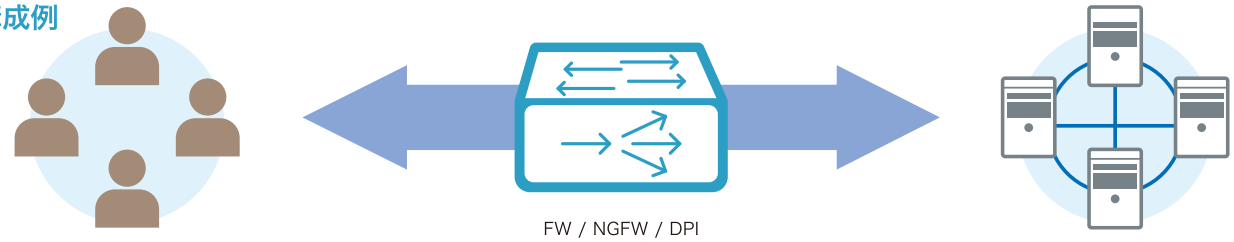
結果レポート：
マルウェアをブロックしパフォーマンスが劣化
設定した閾値を満たさない結果で不合格判定

アドバンスド ミックス トラフィック試験

ミックスプロトコル試験機能に加えて、ロードバランサやプロキシ試験構成など、よりリアルで複雑な環境下での試験を実行することが可能です。また、リモートワーク環境で採用されるVPN（IPSec、SSL）トンネル内で、各種アプリケーションをジェネレートすることが可能です。

■実環境に近いトラフィックの生成が可能
-サブネット単位でアプリケーションシナリオを指定
-アクション編集機能
-TCP上のアプリケーションシナリオをover SSLに設定
■内部DNS機能により、実DNSがない環境でも、宛先の名前（URL）を内部的に解決
■ワンアーム試験機能により、サーバーに対する試験が可能
■試験実行中に、負荷量を変更するデバッグ機能により、測定対象の様子に合わせて即座に試験内容を変更可能
■自動ピークサーチ機能により、最大スループットを即座に確認可能

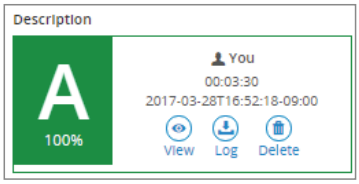
□構成例



□試験例


サブネットとアクションを簡単にアジャスト


コネクション/秒やコネクション同時接続試験をモニタ

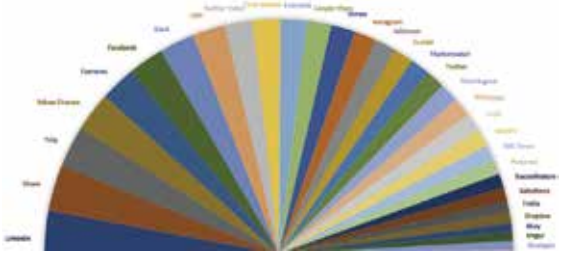


結果レポート：合格/不合格表示

業界標準：NetSecOpen試験対応！

NetSecOpenとは、ネットワークセキュリティベンダ、ツールベンダ、ラボおよび企業が協力してオープンで透過的なテスト標準を作成するネットワークセキュリティ業界標準グループです。CyberFloodはNetSecOpenシナリオを使った試験も可能です。

NetSecOPEN



Underwriters Laboratories Inc.　iol InterOperability Laboratory　EANTC

セキュリティ試験

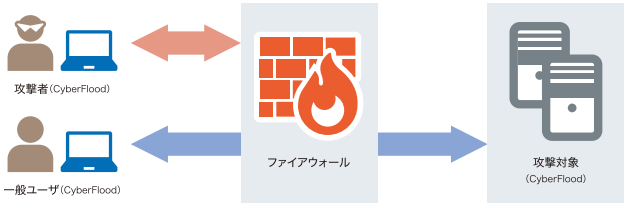
マルウェア検知/脆弱性評価試験

マルウェアや攻撃を擬似することが可能です。サンドボックスやIPS/UTMなどといったセキュリティ製品の検知性能を正しく評価するためにシーケンシャルなやり取りを擬似したリアルなシナリオを提供しています。シナリオはクラウドサービスにより、定期的に更新しています。

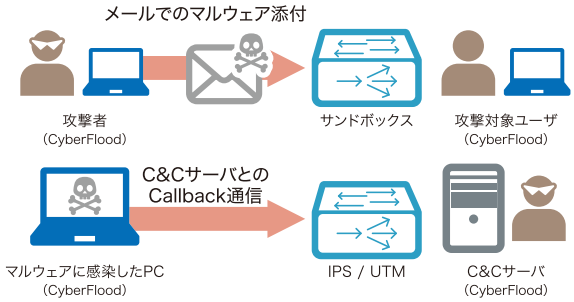
■正常トラフィックとの混在や、任意のタイミングでの送信が可能
■独自プロトコルに対する攻撃トラフィックはpcapインポートやシナリオ編集機能により作成が可能

□構成例

＜脆弱性評価試験＞
■CVE、Secunia、BugtraqのID、深刻度、公開年月などにより分類された攻撃シナリオ　※ID番号を検索キーワードとして利用可能



＜マルウェア検知評価試験＞
■マルウェア検体を含むトラフィックや感染したPCのふるまい（C&CサーバとのCallback通信）を擬似
■マルウェアごとの検知可否や検知率を自動測定



□試験例

半月に1度更新される
アタックシナリオ

各種シナリオ読み込み

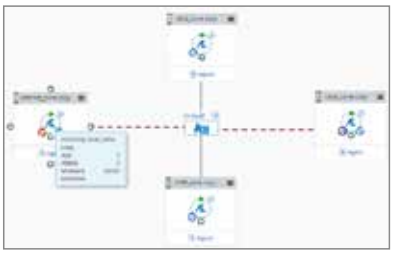
各行攻撃シナリオの
成功・失敗
各シナリオのCV番号や
詳細内容表示

アドバンスド セキュリティ試験

試験のネットワークトポロジを描きながら、マルウェア検知/脆弱性評価試験の設定を作成できます。また、初心者でも簡単に高度な攻撃の擬似が可能です。

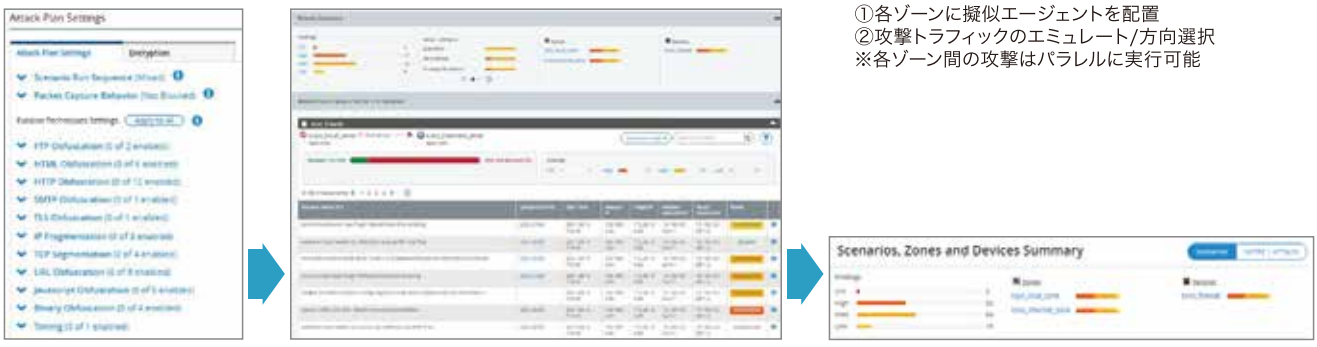
■初心者でもハッカーライクな攻撃擬似が可能
-フレームワーク攻撃診断（P7 コラム参照）　-データ損失防止（DLP）診断
-エバージョンテクニック（嫌がらせのプラン）の擬似　-シナリオの over SSL
■ネットワークトポロジを自由に作成でき、複数Zoneの設定や、複数攻撃可能
■試験予約機能により、深夜試験の自動実行や、定期的な試験の実行が可能

□構成図（トポロジーマップ作成例）



①各ゾーンに擬似エージェントを配置
②攻撃トラフィックのエミュレート/方向選択
※各ゾーン間の攻撃はパラレルに実行可能

□試験例



エバージョンテクニック
パターンマッチによる検知を
防ぐ嫌がらせのオプション

リアルタイムに試験結果を確認

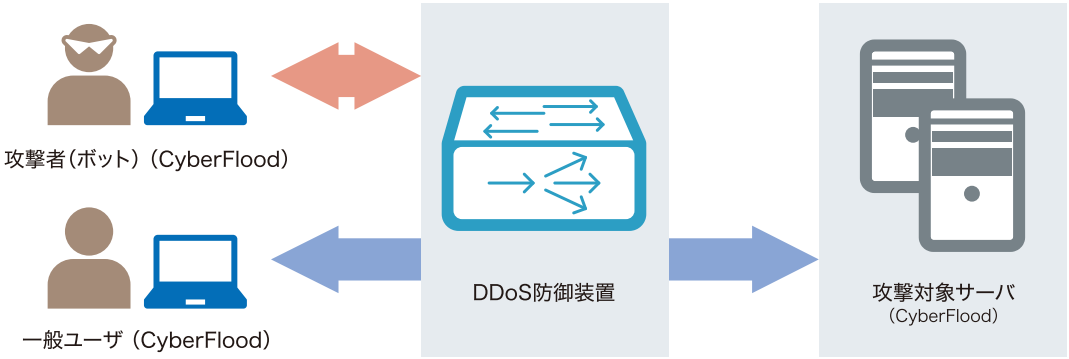
CVEの4段階レベルでの判定結果

DDoSパフォーマンス試験

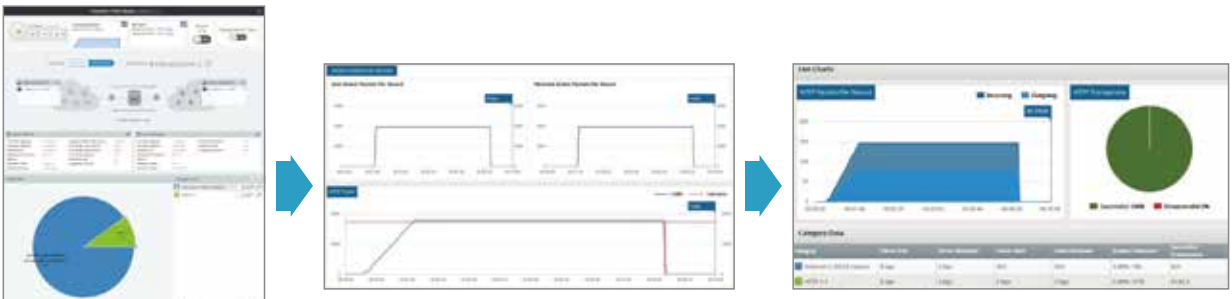
帯域を占有するボリューム型攻撃である、DDoS攻撃の擬似が可能です。DDoS防御装置に対する評価においては多様な攻撃手法に対応するだけでなく、攻撃防御機能による正常通信への影響に関してもパフォーマンス測定における重要な項目といえます。

■正常通信とDDoS攻撃通信の混在試験により、混在環境状況におけるDDoS攻撃の緩和状況や正常通信への影響測定が可能
■リアルタイムチャートにより測定結果を即時に確認可能

□構成例



□試験例



Volumetric DDoS設定画面
攻撃トラフィックと正常通信
トラフィックを混ぜて試験可能

ライブチャート
アタックした数と受信した数を比較

ライブチャート
トラフィックは正常か、DDoSアタック各種カウンタ

フレームワーク攻撃診断（MITRE ATT&CK™※ ,NetSecOPEN）

アドバンスドセキュリティ試験では、MITRE ATT&CKや、NetSecOPENで定義されているフレームワーク（サイバー攻撃の流れと手法を体系化した）のパターン攻撃も可能です。
CyberFloodは約100グループ（2021年8月現在）の有名なハッカー集団の手口を選択して試験を実行することができます。

攻撃者の攻撃方法や行動、目的を明文化したMITREフレームワークの
カテゴリから選択していきながら、シナリオ選択可能

有名なハッカー集団が行う手口からシナリオを選択可能

※MITRE ATT&CK™とは：米国政府の支援を受けた非営利の研究団体の名称で、
世界共通で使われている脆弱性識別子「CVE」を採番している非営利団体です

Avalanche とは

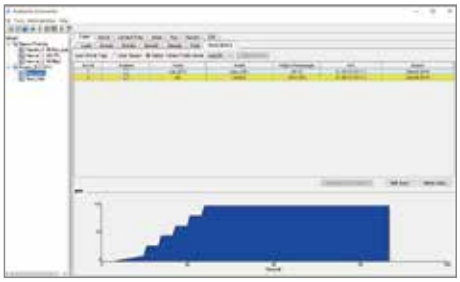
https://www.toyo.co.jp/ict/products/detail/avalanche.html

設定項目が豊富で、クライアントのリクエスト文やサーバーの応答内容、負荷量のかけ方などを任意に設定し、スループット、CPS（コネクション/秒）、TCP同時接続数試験を行うことができます。

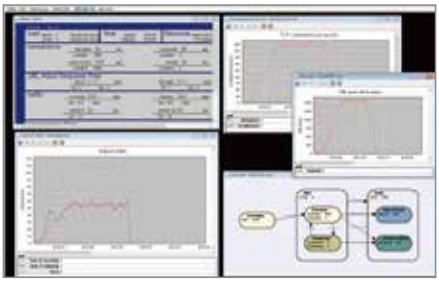
主な特長

-HTTP/HTTPSトラフィック擬似
-変数設定機能
-SAPEE（リプレイ機能）

専用アプリケーションから、よりリアルなアクションや負荷調整をじっくりと設定！


負荷量設定画面

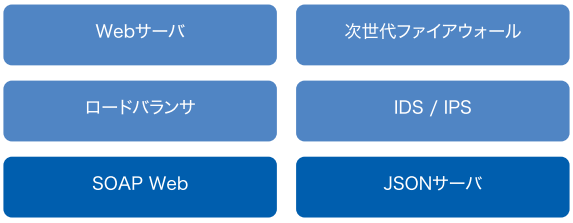

アクションリスト・シナリオ作成画面


試験結果

HTTP/HTTPS

HTTP試験

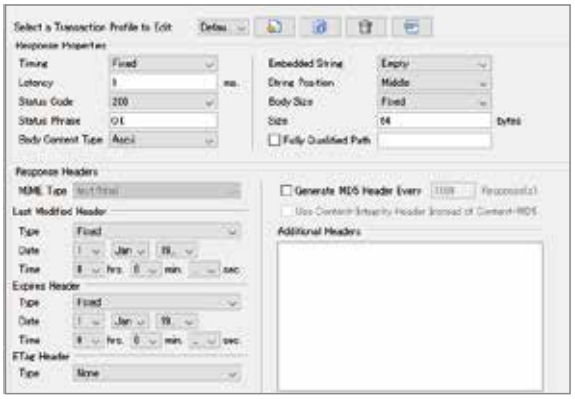
HTTP（HTTPS）試験は、RFC3511で規定されたコネクション/秒、トランザクション/秒、同時コネクション接続数、スループット試験などのベンチマークテストをはじめ、変数設定やサーバコンテンツ設定機能を併用した試験を実行可能です。Avalancheの特長として、クライアント側とサーバ側のTCP・アプリケーションスタックが独立しているため、複雑な試験構成、試験内容を実行することができます。



HTTP試験対象例

コンテンツサーバ擬似

コンテンツ（アスキーデータ、バイナリデータ、ファイル）やコンテンツサイズの指定が可能。更にレスポンスヘッダの編集、ランダム文字列（位置）の挿入、MIMEタイプを設定することにより、コンテンツサーバ擬似のリアリズムを追求し、アプリケーション・アウェアのネットワーク機器の評価が可能になります。


トランザクション・サーバコンテンツ作成画面

プロキシサーバ試験

アプリケーションごとに別々のプロキシサーバに接続できます。

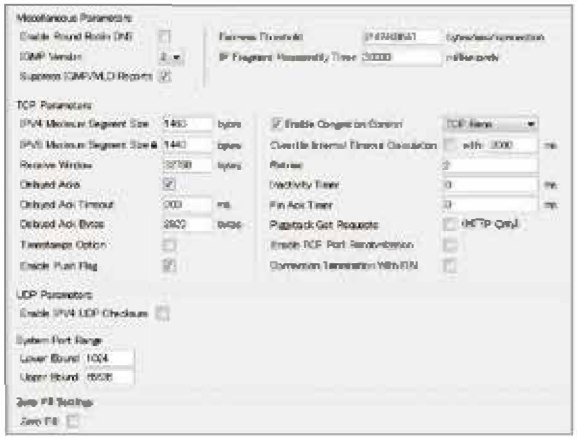

プロファイル・プロキシサーバ設定画面

Web高速化プロトコル（SPDY,HTTP/2,HTTP/3）

Web表示の高速化を目的として策定されたSPDY、HTTP/2、HTTP/3をサポートすることにより、リアリズムのあるブラウザエミュレーションが可能となります。

トランスポートのリアリズム

専用測定器として、信頼あるNICドライバを搭載しています。また、TCPパラメータや輻輳制御アルゴリズムの選択も可能となっています。これらの機能を使用し、テストオペレータは、TCPパラメータを変更しながらネットワーク機器のふるまいを確認できます。



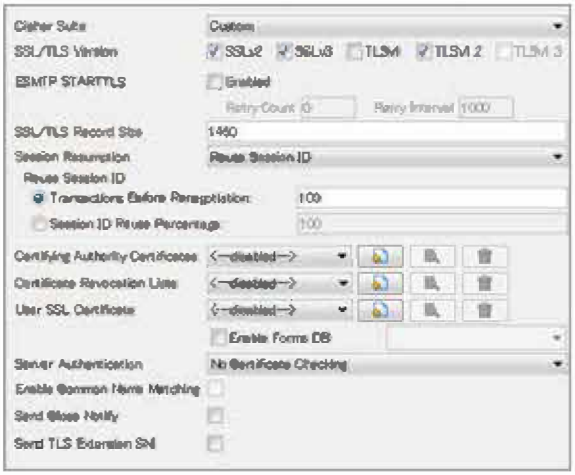
ネットワーク・TCP/UDPパラメータ設定画面

SSL / TLSプロファイル

AvalnacheSSL/TLSテスティングの特長として、クライアント・サーバにそれぞれのサイファスイートが設定できます。

■クライアントプロファイル
クライアントプロファイルでは、クライアント証明書、CA証明書、CRLのインポート、SNI(Server Name Identification)の設定が行えます。

■サーバプロファイル
サーバプロファイルでは、サイファスイート、サーバ証明書、CA証明書、CRLのインポート、SNI(Server Name Identification)の設定などが行えます。



SSL/TLS設定画面

変数設定機能

アプリケーションテスティング

複雑なトランザクションが必要となるWebサーバテスティングや、アプリケーション・アウェアのネットワーク機器の評価が可能になります。

■ブラウザオプション
サーバから指定されたリダイレクト先へHTTPリクエストを送ること、クッキー付与などが可能になります。

■Dynamic Variable機能
Avalancheが送るリクエストの内容を動的に変更することができます。

※ユーザ名など、リクエストごとに変更させたい内容をCSV形式で登録しておくことができます。
※セッションIDなどの試験実行前には特定できないデータの場合、サーバからの応答内容をサーチしてリクエスト内容を動的に変更することができます。
※リクエスト内容にランダムな数値、文字列を含ませることができます。

■Content Validation機能
HTTP, HTTPSの試験において、サーバから返された応答内容にユーザが指定した文字列が含まれている、もしくは含まれていないことをチェックできます。その結果によって試験自体の停止やそれ以降のリクエストを停止することができます。Sorryページ、Errorページ、Webサイトへのログインの失敗などのチェックに有効です。

■SearchCriteria機能
セッションIDなどの、試験実行前に特定できないデータを、サーバからの応答内容からサーチして、変数に代入し、ActionList内でその内容を使用することにより、Avalancheの送出するHTTPリクエスト内容をサーバの応答内容に応じて動的に変更させることができます。

SOAP Web試験、JSON試験

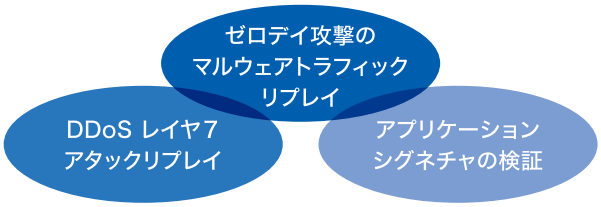
GET/POSTリクエストに任意のデータを使用できます。サーバからのレスポンスによりXMLデータを動的に変更し、SOAP Web試験やJSON試験に応用できます。

アクション・HTTPコンテンツ設定画面

SAPEEオプション トラフィックリプレイ(SAPEE)

SAPEEとは

SAPEEはTCP / UDP上で動作するすべてのアプリケーショントラフィックのプレイバックを実現します。また、マルチセッションをサポートしており、P2PやMessengerプロトコルの再現ができます。



SAPEEの特長

-IPv4 / IPv6でのTCP / UDPアプリケーションのプレイバック
-P2Pなどのマルチセッションを使用するアプリケーションも再現
-プレイリストセッションのスタートタイミング、順番を変更可能
-ライブラリでのアプリケーションpcapの提供
-ライブラリはメーカサイトよりダウンロード可能
-任意アプリケーションの増幅が可能
-パケットシーケンス、方向、パケット間ディレイを変更可能
-FormDBライクな変数値によるマルチユーザトランザクション
-ユーザカスタムのTCP / UDPベースのプロトコルを作成可能
-ペイロード内のデータを任意にカスタマイズ

SAPEEで使用するリプレイトラフィック

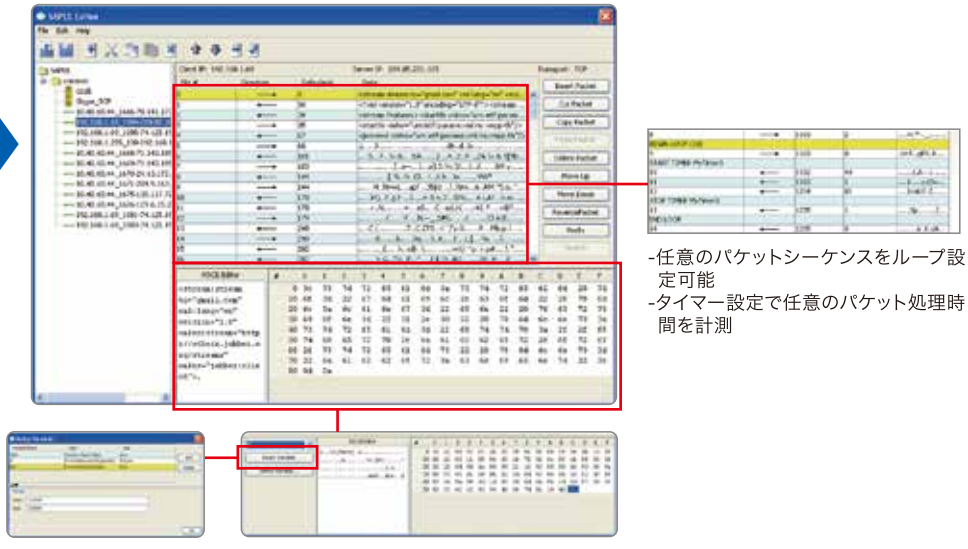
SAPEEで使用するアプリケーションリプレイトラフィックは、
次の3つから選択できます。
-プレビルドされたアプリケーションリストから選択
取込み済みのプロトコル:
Bit Torrent, Gnutella, MSN, Yahoo, Skype, SQL, MYSQL, Gtalk, Oracle, SMB, NFS, Remote Desktop, Exchange, LDAP, uTorrent
-ユーザが保有するpcapファイルをインポート
(最大ファイルサイズ約200MBまで)
-Spirent Communicationsデータベースよりダウンロード

プレビルドされたアプリケーションリスト

SAPEEの機能

SAPEEでは、プレイリストによりアプリケーショントラフィックを再現します。ストリームごとにサーバIPの設定やタイマー設定ができます。ストリームに含まれるパケットのシーケンスは変更ができ、ループ設定や計測用のタイマー設定もできます。また、パケットペイロードの値も編集できます。

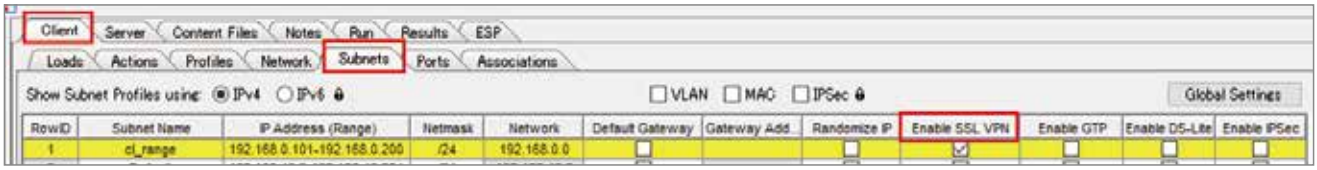

-任意のpcapファイルをインポート可能
-ウィザードでリプレイプロファイル、サーバ設定など一括で設定可能


-任意のパケットシーケンスをループ設定可能
-タイマー設定で任意のパケット処理時間を計測
-ペイロードに任意の値入力可能
-FromDBライクな機能で擬似ユーザ毎に異なる値を挿入可能

その他の機能

SSL-VPNクライアント擬似

リモートワーク環境で採用されるSSL-VPN環境のクライアントの擬似が可能です。
（シスコシステムズ合同会社 Cisco AnyConnect Secure Mobility Client™、パロアルトネットワークス株式会社 Global Protect™）



SSL-VPN設定画面　1つのVPN内で、複数のプロトコルのアクションをジェネレートすることが可能です。

メール（SMTP / IMAP4 / POP3）

Avalancheのメールオプションでは、クライアント擬似・サーバ擬似をそれぞれ単独で行えます。クライアントのアクションリストに記載されたコマンドでメール配送やメールBoxの検索・メール取得が行えます。また、サーバプロファイルでメールBoxを擬似することもできます。

■SMTP

-クライアント擬似をし、SMTPプロトコルを使用したMTA（Message Transfer Agent）への負荷試験が可能
-クライアント・サーバ両方を擬似した、メールプロキシゲートウェイの評価が可能
-添付ファイル・MIMEタイプは任意に設定可能
-STARTTLS、STMP Authenticationにも対応
-4つの認証方式をサポート：PLAIN, LOGIN, CRAM-MD5, Digest MD5
-送信可能なESMTP アクション：RSET, EHLO, SOML, SEND, SAML, VRFY, EXPN, HELP, TURN, ETRN, XXXX

■IMAP4

-クライアント擬似をし、IMAP4プロトコルを使用したメールboxへの負荷試験が可能
-クライアント・サーバ両方を擬似した、メールプロキシゲートウェイの評価が可能
-コマンドサポート一覧:LOGIN, CAPABILITY, NOOP, SELECT, CHECK, CLOSE, EXPUNGE, STATUS, LIST, FETCH_BODY, FETCH_HEADERS, STORE, LOGOUT

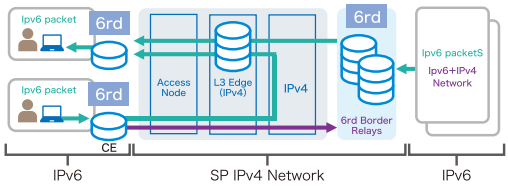
■POP3

-クライアント擬似をし、POP3プロトコルを使用したメールboxへの負荷試験が可能
-クライアント・サーバ両方を擬似した、メールプロキシゲートウェイの評価が可能
-コマンドサポート一覧：RETR, CHECK, STAT, LIST, UIDL, DEL

IPv6移行化技術

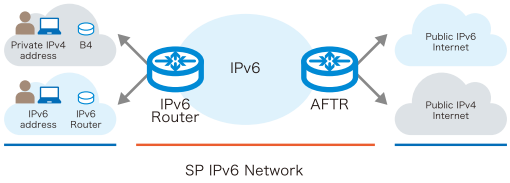
6RD　IPv6 over IPv4

Avalancheのクライアントテストポートは、6RDのCE機器と宅内のIPv6端末を擬似します。ステートレスなアドレス変換が必要な6RD Border Routerの評価を行います。



DS-Lite

Avalancheのクライアントテストポートは、CE機器であるB4（Basic Bridging Broadband）と宅内のIPv4端末を擬似します。CGNでNATされるIPv4トラフィックを印加し、AFTR（Address Family Transition Router）の性能評価を行います。



製品ラインアップ

C200

最も高パフォーマンスなハードウェアモデルながら、1Uサイズの省スペースモデルです。

サイズ	1U 445（W）x947（D）x 43（H）mm
重量	11kg
電源仕様	100-240V,50/60Hz,1600W
CyberFloodコントローラ	筐体内蔵

C100-S3-MP

ハイパフォーマンスハードウェアモデルで、100G～1Gまで幅広いインターフェースをサポートしています。

■ハードキャリーケースオプションあり
サイズ：53（W）x 29（D）x 60（H）cm

サイズ	3U 420（W）x502（D）x133（H）mm
重量	14kg
電源仕様	115-230V,50/60Hz,750W
CyberFloodコントローラ	外部サーバー（別途ご用意ください） 動作環境はCyberFlood Virtualと同様

CF30

1Uサイズのミドルパフォーマンスハードウェアモデルです。
中規模のネットワークの性能測定に最適なモデルです。

サイズ	1U 437（W）x399(D)x43(H)mm
重量	8.16kg
電源仕様	100-240V,50-60Hz,600W
CyberFloodコントローラ	筐体内蔵

Spirent C1

L2-L7まで対応している小型All-in-Oneアプライアンスです。

■Spirent TestCenter機能同梱
■小型、持ち運び可能

サイズ	331（W）x254（D）x89（H）mm
重量	4.5kg
電源仕様	115-240V,50/60Hz,300W
CyberFloodコントローラ	外部サーバー（別途ご用意ください） 動作環境はCyberFlood Virtualと同様

Spirent CF400

New

サイズ	2RU 437（W）×574（D）×89（H）mm
重量	15.6 kg
電源仕様	100-240 Vac, 50/60Hz, 2000W
CyberFloodコントローラ	筐体内蔵

CF400/C200/C100-S3-MP 共通 100G 筐体用アクセサリ

-10G ファンアウト：DAC ブレークアウトケーブル
(IX QSFP+ TO 4X10G SFP+), QSFP＋トランシーバ、
ブレークアウトケーブル (MPO TO 4XLC)
-25G ファンアウト：QSFP28 トランシーバ、
ブレークアウトケーブル (MPO TO 4XLC)
-40G モード：DAC ケーブル (IX QSFP+ TO I X QSFP+),
QSFP＋トランシーバ (40GBASE-SR)
-100G モード：DAC ケーブル (IX QSFP28 TO IX QSFP28),
QSFP28 トランシーバ (100GBASE-SR4 / LR4)

ハードウェアモデル比較

	CF400	C200	AvalancheC100-S3-MP								CF30			Spirent C1			
型番	CF-KIT-00x-CF400	KIT-00x-C200	AKIT-042	AKIT-021	AKIT-022	AKIT-023	AKIT-024	AKIT-025	AKIT-026	AKIT-027	AKIT-028	CF-KIT-001-CF30	CF-KIT-002-CF30	CF-KIT-003-CF30	KIT-01-20XX	KIT-01-BASE	KIT-03-20XX	KIT-03-BASE
100G QSFP+/QSFP28※1	8	4	4	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
40G QSFP+/QSFP28※1				—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
10G SFP+※1	—	16※2	16※2	8	8	4	4	—	—	8	4	8※3	8※3	8※3	—	—	2	2
1Gb SFP	—	—	—	—	—	—	16	—	16	8	—				—	—	—	—
10/100/1000Base-T ネイティブポート	—	—	—	—	8	16	—	16	—	—	—	—	—	—	4	4	4	4
SSLカード	—	○ (2枚)	※4	※4	※4	※4	※4	※4	※4	※4	※4	×	×	×	×	×	×	×

※1.100G/40G/10Gは排他的です　※2.ブレイクアウトケーブル利用時　※3.10Base-T、100Base-TX未対応　※4.オプションで追加可能

CyberFlood Virtual/Avalanche on CyberFlood Virtual

CyberFlood Virtual は、サーバ仮想化環境でのアプリケーションレイヤ試験を実現する仮想アプライアンスモデルです。仮想マシン上で動作し、クライアント / サーバ間のアプリケーショントラフィックをエミュレートすることで、サーバ仮想化環境のアプリケーション性能を評価できます。プライベートクラウド、パブリッククラウドどちらにも対応した仮想アプライアンスモデルです。
また、同じプラットフォーム上でモードを切り替えることで、Avalancheとしてもご利用いただけます（Avalanche on CyberFlood）。

■パフォーマンスモデル
-サーバーのリソースを最大限に使い、高負荷をかけることができる仮想アプライアンスモデル

■ファンクショナルモデル
-1Gbpsの制限がかかった機能試験向けの仮想アプライアンスモデル　-性能上限：1Gbps throughput / 15k CPS / 100k 同時接続数

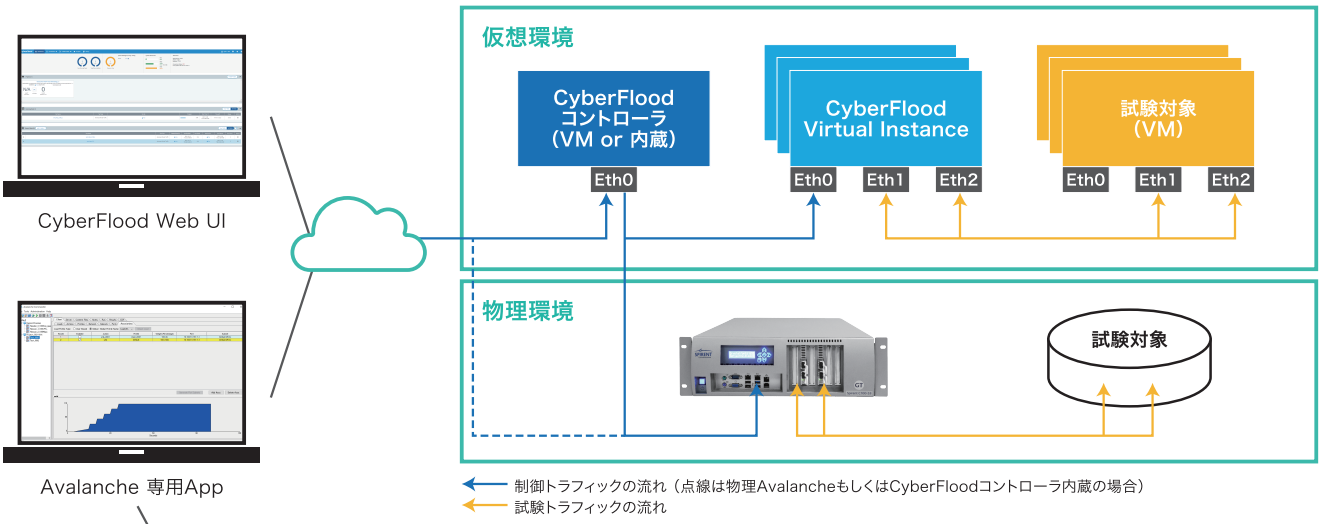
■動作環境

仮想環境	コントローラー※4				バーチャルポート			
	CPU/v CPU※3	メモリ[GB]	HDD[GB]	インスタンスタイプ	CPU/v CPU	メモリ[GB]	HDD[GB]	インスタンスタイプ
ESXi	最小：2vCPU 推奨：4vCPU	最小：16 推奨：24	最小：160 推奨：320	VMWare ESXi 6.5, 6.7, 7.0	4vCPU以上、36vCPU下/VM (ライセンスに準ずる)	1vCPUあたり2GB以上	20GB	VMWare ESXi 6.7, 7.0, 8.0
KVM	最小：2vCPU 推奨：4vCPU	最小：16 推奨：24	最小：160 推奨：320	Ubuntuバージョン 20.04 Linuxベースの他のOSもサポートしています。詳細はお問合せください。	4vCPU以上、36vCPU下/VM (ライセンスに準ずる)	1vCPUあたり2GB以上	20GB	Ubuntuバージョン 20.04 Linuxベースの他のOSもサポートしています。詳細はお問合せください。
AWS	※1			t2 .xlarge	※1※2			c5n.*
Azure	最小：2vCPU 推奨：4vCPU	最小：16 推奨：24	最小：160 推奨：320	詳細はお問合せください。				Standard_D8s_v5 Standard_D16s_v5
GCP	※1			n1-standard-4				n2-standard-16 n4-standard-16

※1：インスタンスの仕様をご確認ください。
※2：4vCPU以上、36vCPU以下/VMのインスタンスを使用してください。（ライセンスに準ずる）
※3：64bit版をご使用ください。
※4：コントローラーをブラウザで表示する際は、GoogleChromeかFirefox最新版をご使用ください。

接続構成例

CyberFloodはブラウザベースのWebUI、Avalancheは専用アプリケーションからシナリオの作成、実行を行います。また、CyberFloodをご利用の場合には、CyberFloodコントローラが必要です（一部モデルは筐体内蔵）。Virtual環境と、物理アプライアンスの環境がIPリーチャブルであれば、下記のように組み合わせた構成も可能です。



■制御用PCの必要条件

-LAN：10 / 100 / 1000Base-T：1 ポート　-CPU：E6400 Intel® Core™ 2 CPU（同等またはそれ以上）
-RAM：4GB 以上　-ハードディスク：空き容量 40 GB 以上
-OS： Windows 10 (Ver 4.63以降)、 Windows 11 (Ver5.39以降)
-ブラウザ：Google Chrome（最新バージョン）, Mozilla Firefox（最新バージョン）　※CyberFlood WebUI用

CyberFlood/Avalancheパフォーマンス

	Avalanche/CyberFloodパフォーマンス						
モデル名 / 試験項目	CF400 8×100G	C200 4x100G	C100-S3-MP 100G×4	C100-S3-MP 10G×8	CF30 10G×8	C1 10G×2	CFv
SSLカード/ライセンス	あり	あり	あり	あり	あり	なし	パフォーマンス ライセンス※3
HTTP1.1 コネクション/秒	3,450,000	1,990,000	1,270,000	1,040,000	1,090,000	189,000	208,000
HTTP1.1 リクエスト/秒	6,620,000	4,200,000	2,570,000	2,150,000	2,350,000	407,000	414,000
HTTPS1.1 セッション/秒 TLSv1.2 (AES128-GCM-SHA256)	437,000	219,000	145,000	128,000	126,000	20,000	21,000
HTTP1.1 同時接続	320,000,000	103,000,000	83,300,000	74,300,000	81,800,000	1,100,000	649,000
HTTPS1.1 同時接続 TLSv1.2 (AES128-GCM-SHA256)	8,020,000	2,550,000	2,060,000	1,840,000	2,040,000	25,000	16,000
HTTP1.1 帯域 (kbps)	393,000,000	188,000,000	168,000,000	39,300,000	39,300,000	8,990,000	9,820,000
HTTPS1.1 帯域 (kbps) TLS1.3 (AES128-GCM-SHA256)	250,000,000	77,800,000	69,300,000	39,300,000	39,300,000	9,310,000	9,750,000

※試験シナリオによってパフォーマンスは変動します。※コントローラが含まれる筐体でも外部コントローラを使用して測定しています。
※CFvはリソースが十分に確保された場合の最大値です。

CyberFloodオプションライセンス　Avalancheオプションライセンス

CyberFloodオプションライセンス

ベースライセンス	HTTP Throughputテスト +グローバルIP トラフィックセレクタ
	HTTP Connections per Secoundテスト +グローバルIP トラフィックセレクタ
正常系テストライセンス	DNS テストメソドロジー +グローバルIP トラフィックセレクタ
	THROUGHPUT with MIXED TRAFFICテスト +テストクラウド アプリケーション コンテンツ +グローバルIP トラフィックセレクタ
	HTTP OPEN CONNECTIONS テスティングメソドロジー +グローバルIP トラフィックセレクタ
攻撃系テストライセンス	Cyber Securityスイート +アタックコンテンツ +アドバンスドマルウェアコンテンツ
	ボルメトリック DDoS/プロトコル DDoS
トラフィックリプレイ機能	トラフィックリプレイ
オプション機能ライセンス	アドバンスド ミックスドトラフィックアセスメントライセンス +グローバルIP トラフィックセレクタ

※正常系試験ライセンスバンドル内容：ベースライセンス+正常系テストライセンス+トラフィックリプレイ機能　※テストクラウドコンテンツは含まれておりません
※攻撃系/正常系試験ライセンスバンドル内容：上記オプション機能ライセンス以外全て
※+マークは別購入可能な、サブスクリプション形式のオプションライセンスです

Avalancheオプションライセンス

ベースライセンス

C100MPS3/C1	HTTP, DNS ,FTP, TELNET
C200/CF30	HTTP, HTTPS, DNS, FTP ,TELNET

バンドル版ライセンス

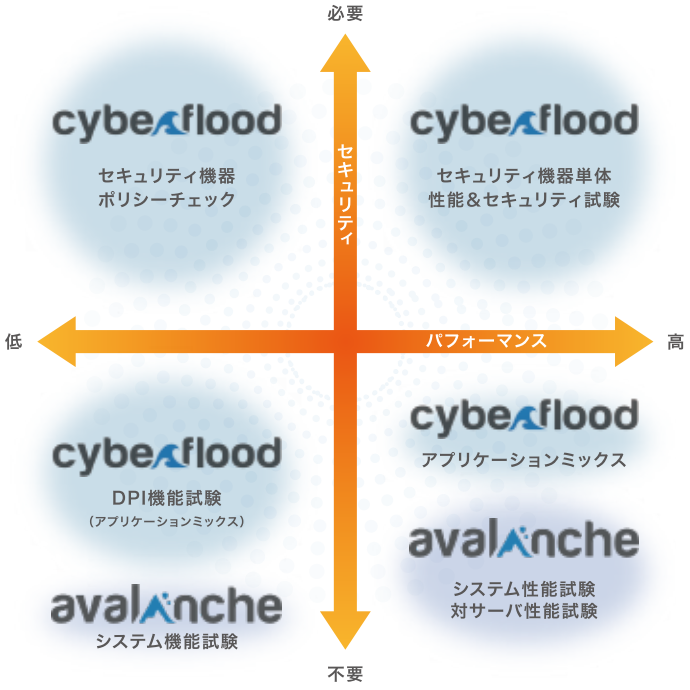
アプリケーション テスティング ソフトウェア バンドル	Enhanced HTTP, Application testing, SSL
セキュリティ　ソフトウエア　バンドル	IPSec, Radius, 802.1x/NAC
トリプルプレイ プロトコル ソフトウェア バンドル	PPPoE, SIP, RTSP/RTP, Real, Windows Media, VoD, Mail, SAPE
アクセス テスティング ソフトウェア バンドル	PPPoE, DHCP, SAPEE
エクステンディド アプリケーション ソフトウェア バンドル	SAPEE, アプリケーションテスティング, EnhancedHTTP,Vulnerability Assessment/DDoS
ナレッジベース ソフトウェア バンドル	Vulnerability Assessment/DDoS, SAPEE, ナレッジベースアップデートサブスクリプション 1年間

個別ライセンス

カプセル化プロトコル		DS-LITE				GTP SGSN-GGSN			
ネットワークアクセスプロトコル		DHCP	IPSEC	SSL	PPTP	PILOT※1	PPPoE	IPv6	6RD
認証プロトコル		802.1X NAC				RADIUS			
アプリケーションプロトコル	データプロトコル※	HTTP2		HTTP3(QUIC)		SPDY			
	メールプロトコル	EMAILOVER SSL (SMTP, POP3, IMAP含)				MAIL (SMTP POP3 IMAP4含)			
	ファイルアクセスプロトコル	CIFS				NFS			
音声・メッセージ&ビデオプロトコル		SIP	ABR ビデオストリーミング	MM4 (マルチメディア メッセージング SVC MM4)		RTMP	VOD (ビデオ オンデマンド マルチキャスト)	UNIC (ビデオ ストリーミング ユニキャスト)※2	
その他の機能		APP (アプリケーション テスティング) ※3		ESP※4		SAPEE※5	VAD(脆弱性評価)/DDoS		

※1 PPTP PROTOCOL PILOT PACKET　※2 RTP/RTSP , Real , Windows含　※3 Webサービス、ERP、SpirentAvalancheのアプリケーションを使用したCRMアプリケーション、Cookie、セッションID、動的をサポートするテスト機能リンク、自動フォローリダイレクト、追加ヘッダー、コンテンツ検証、SOAPメッセージ、思考時間、変数思考時間、変数の割り当て含　※4 背景負荷　※5 PCAPファイルプレイバック機能

CyberFloodとAvalancheの棲み分け



Spirent SecurityLabs

https://www.toyo.co.jp/ict/products/detail/Spirent_SecurityLabs.html

Spirent社のSecurityLabsは米国の経験豊かなホワイトハッカーチームがIoTデバイス、ネットワーク、アプリケーションのセキュリティリスクを診断するペネトレーションテストサービスです。診断には単純なツールによるスキャンだけではなく、多くのマニュアル診断、得られたリスクのスコアリング、緩和策が含まれます。

■サービス対象

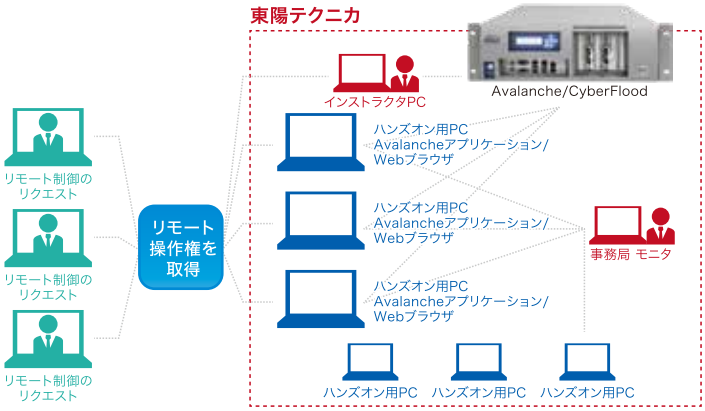
-Webアプリケーション / サービス　-モバイルアプリケーション
-ネットワーク&無線　-組み込みデバイス
-IoTデバイス / Automotive(CANBUS、車載イーサネット) / 制御システム(SCADA)

securitylabs

ハンズオンセミナー

Spirent Avalanche/CyberFloodを最大限にご活用いただくために、ハンズオンセミナー(無償)を当社セミナールームで定期開催しております。オンラインによるリモートハンズオンセミナーも開催しております。初めてご使用される方向けにサーバーや、ロードバランサー等のネットワーク機器の負荷試験/セキュリティ試験の設定方法や、解析ポイント、Tipsをハンズオン形式でレクチャします。日程や詳細内容は当社Webページをご覧ください。

東陽テクニカ　ハンズオンセミナー



株式会社 東陽テクニカ　情報通信システムソリューション部

〒103-8284　東京都中央区八重洲1-1-6
TEL.03-3245-1250（直通）　FAX.03-3246-0645　E-Mail : ict_contact@toyo.co.jp
www.toyo.co.jp/ict/

大阪支店	〒532-0003 大阪府大阪市淀川区宮原1-6-1（新大阪ブリックビル）	TEL.06-6399-9771	FAX.06-6399-9781
名古屋支店	〒460-0008 愛知県名古屋市中区栄2-3-1（名古屋広小路ビルヂング）	TEL.052-253-6271	FAX.052-253-6448
宇都宮営業所	〒321-0953 栃木県宇都宮市東宿郷2-4-3（宇都宮大塚ビル）	TEL.028-678-9117	FAX.028-638-5380
R&Dセンター	〒135-0042 東京都江東区木場1-1-1	TEL.03-3279-0771	FAX.03-3246-0645

ISO 14001 JQA-EM4908
ISO 9001 JQA-QM8795 技術センター

※本カタログに記載された商品の機能・性能は断りなく変更されることがあります。
※本カタログに記載されている社名・ロゴは各社の商標及び登録商標です。各社の商標及び登録商標はそれぞれの所有者に帰属します。

CAW20241113-TOYR6