FOR IMMEDIATE RELEASE
即日発表

SPIRENT EXTENDS SECURITY AND PERFORMANCE TESTING LEADERSHIP WITH CYBERFLOOD UPDATE
SPIRENT CYBERFLOOD のアップデートによりセキュリティーおよびパフォーマンス試験のリーダシップを拡大

Industry's First Server-Response Fuzzing Raises Security Standards for Testing Against Malicious Attack Vectors
業界初のサーバーレスポンス・ファジングで、悪意ある攻撃ベクター対策試験向けセキュリティー標準を引き上げ

RSA 2017, SAN FRANCISCO, Calif., February 13, 2017 – Spirent Communications plc (LSE:SPT) today extended its lead in security and performance testing by introducing the industry's first server-response fuzzing capability within CyberFlood, its premier security test solution. A breakthrough in security and performance testing, CyberFlood's server-response fuzzing functionality tests the ability of security devices—firewalls, intrusion prevention systems (IPS), secure web gateways and others — to handle malformed traffic sent from a server on the Internet to a client device using a single test solution. This is achieved without the time, effort and cost of building a complex test environment, allowing the user to get up and running more quickly with better results than ever before.

RSA 2017、カリフォルニア州サンフランシスコ、2017 年 2 月 13 日 – Spirent Communications plc（LSE：SPT）は本日、業界初のサーバーレスポンス・ファジング能力を備えた CyberFlood とその優れたセキュリティー試験ソリューションを発表し、セキュリティーおよび性能試験業界におけるリードをさらに広げました。まさにセキュリティーおよび性能試験におけるブレークスルーと言えます。CyberFlood のサーバーレスポンス・ファジング機能は、セキュリティー機器（ファイアーウォール、侵入防止システム（IPS）、セキュア Web ゲートウェイなど）がインターネット上のサーバーからクライアント機器に送られる不正なトラフィックを処理する能力を、単一のテストソリューションを使用することにより試験します。複雑なテスト環境を構築するための時間・

労力・費用をかけることなく、これまで以上に優れた結果をより迅速に得ることができます。

“We launched CyberFlood last year with SmartMutation™, the first-of-its-kind, true intelligence-driven fuzzing strategy. This set a new benchmark for security testing, allowing testing to go deeper, wider and across more code paths than any other solution in the industry,” said David DeSanto, director, products and threat research at Spirent Communications. “Other fuzzing solutions today only offer users the ability to fuzz the client definition of the network protocol when testing a device.

Spirent Communications 製品/脅威リサーチ担当ディレクター David DeSanto 氏の話
「私たちは昨年、最初の真のインテリジェンス主導型ファジング技術である SmartMutation™とともに CyberFlood を発売しました。セキュリティー試験の新たなベンチマークを打ち立て、業界内の他のソリューションよりも深く、広く、そしてよりコードパス横断的な試験を実現しています。現在その他のファジングソリューションでは、デバイスをテストする際に、ネットワークプロトコルのクライアント定義しかファジングできません」

“Leveraging CyberFlood’s unique technology, users can now fuzz the server definition of the network protocol, confirming that a device can handle malformed responses from a server on the Internet targeting a client device, one of the most common and malicious attack vectors leveraged by hackers today. This gives enterprises, service providers and equipment manufacturers a fast and easy way to test security devices with no test environment to set up, and with no false positives during testing”.

「CyberFlood の独自技術を使用することで、ネットワークプロトコルのサーバー定義をファジングすることができ、インターネット上のサーバーから送られるクライアント機器を対象とした不正なレスポンスへの対処を強化することができます。こういったレスポンスは、今日のハッカーが使用する一般的な攻撃ベクターのひとつです。
CyberFlood を使うことで、企業、サービスプロバイダーや機器メーカーは、試験環境を

構築することなく、また誤判定に悩まされることなく、すばやく簡単にセキュリティー機器をテストすることができます」

The latest CyberFlood update includes several new features while enhancing CyberFlood's ease of use:

CyberFlood 最新アップデートは、新たな機能を追加しながら、CyberFlood の使いやすさを高めています。

- New Attacks-Only and Client-Only DDoS attack modes add greater flexibility to DDoS attack emulation and enable customers to quickly go from the login screen of CyberFlood to a large-scale DDoS attack emulation in a few clicks.
  新しい Attacks-Only および Client-Only DDoS アタックモードにより、より柔軟な DDoS アタックのエミュレーションが可能になりました。また、CyberFlood ログイン画面から大規模 DDoS 攻撃エミュレーションまで数クリックで簡単に到達できるようになりました。
- New Network Resiliency tests cover the full range of RFC 2544 verification, including measuring maximum throughput, latency, jitter and burstability.
  新たなネットワーク弾力性テストは、RFC 2544 検査の全範囲をカバーしています。これには、最大スループット、レイテンシー、ジッター、バースト可能性の測定を含みます。
- Tests can be organized in groups focused around a specific goal, such as an upcoming software release or enterprise product evaluation, enhancing collaboration within teams.
  試験は特定の目標（予定中のソフトウェアリリース、企業の製品評価など）に向けたグループ別に組織され、チームの連携を強化します。
- Additional fuzzing protocols allow CyberFlood to test devices across the entire Layers 2 through 7 stack and across multiple industry verticals, including industrial control, healthcare, finance, IoT and automotive.
  追加のファジングプロトコルにより、CyberFlood は Layer2-7 全体の機器およ

び複数の産業（産業制御、ヘルスケア、金融、IoT、自動車など）と垂直関係にある機器を試験することができるようになります。

CyberFlood continues to set the industry standard for malware testing with the only near-zero-day malware offering available in the industry, allowing enterprises to find the holes in their threat landscape, service providers to validate their SLAs and equipment manufacturers to confirm and extend their signature as well as heuristic detection functionality.

CyberFlood はマルウェア試験の業界標準を確立し続け、業界内で有効なニアゼロデイマルウェアを用いたフレッシュな攻撃を提供します。企業は脅威にさらされた状況のセキュリティーホールを見つけやすくなり、サービスプロバイダーは SLA を検証できるようになり、機器メーカーは署名と発見機能性の強化・拡大が可能となります。

“WedgeAMB provides our customers with uncompromising malware prevention by delivering the threat detection accuracy of a sandbox, with the inline, real-time blocking speed of an IPS,” said James Hamilton, CEO at Wedge Networks, Inc., the leader in Orchestrated Threat Management. “CyberFlood’s ability to provide performance and accuracy testing with the freshest, most unique malware testing available in a single solution enables us to continuously evaluate, demonstrate and improve our solutions.”

組織化された脅威管理の先進企業であるWedge Networks, IncのCEO James Hamilton氏の話「WedgeAMBは、IPSのインラインでリアルタイムなブロックスピードとともに、サンドボックスの正確な脅威検出能力を提供することにより、強固なマルウェア予防を顧客に提供しています。CyberFloodが単一のソリューションで実現する最新で独自のマルウェア試験の性能と正確性により、当社のソリューションの継続的な評価、実証および改善が可能となっています」

Spirent at RSA 2017

RSA 2017 の Spirent

CyberFlood v17.1.0 will be on display in the Spirent Communications booth S2015 in the South Hall during the upcoming RSA Conference 2017, being held February 13–17 at the Moscone Center in San Francisco. Spirent will also demonstrate CyberFlood's server-response fuzzing and advanced malware testing capabilities in the booth.

CyberFlood v17.1.0 は、間もなく開催される RSA Conference 2017（2 月 13-17 日、モスコーン・センター、サンフランシスコ）の Spirent Communications ブース（南ホール S2015）において展示されます。ブースでは、CyberFlood のサーバーレスポンス・ファジングおよび優れたマルウェア試験能力の実演を予定しています。

Also at the show, Spirent Positioning Security Technologist Guy Buesnel will present a classroom session on the evolution of deliberate threats to global navigation satellite systems (GNSS). The session, which will be held at 9:00 a.m. on February 17 in Moscone West, will address the evolution of deliberate GNSS threats and present the latest evidence of deliberate jammer use from a network of detector devices.

また、会場では、Spirent のセキュリティー・テクノロジスト Guy Buesnel が、全球測位衛星システム（GNSS）に対する計画的な脅威の発達に関するクラスルームセッションを開催します。このセッションは、2 月 17 日午前 9 時よりモスコーン・ウェストで開催されます。GNSS に対する計画的な脅威の発達をテーマに、探知装置のネットワークから得られた計画的な妨害行為の最新の形跡を紹介します。

About Spirent Communications

Spirent Communications について

Spirent Communications is a leader in assessment, validation and monitoring solutions that test and verify the performance and security of enterprise network and application infrastructures in a broad range of environments, including enterprise, IoT, automotive, mobility and critical infrastructures. Global 2000 customers in government, industry, healthcare, and financial services employ Spirent Security products and services to ensure an unsurpassed

service experience while meeting business objectives of reducing churn, increasing revenue and strengthening market share. For more information about Spirent Security solutions and services, visit www.spirent.com/security.

Spirent Communications は広範な環境（企業、IoT、自動車、モバイル機器、重要インフラなど）における企業ネットワークおよびアプリケーションインフラの性能とセキュリティーを試験・実証する測定・検証・監視ソリューション分野のリーダーです。政府、工業、ヘルスケア、金融サービスの領域で、世界 2000 以上の顧客が、顧客の離脱を防ぎ、収益を増やし、市場シェアを高めるという経営目的を達成しながらサービスエクスペリエンスを確保するために Spirent Security 製品およびサービスを使用しております。Spirent Security ソリューションおよびサービスのより詳しい情報は次のページをご覧ください。www.spirent.com/security

# # #

Media and Analyst Contacts:

	Americas	Asia Pacific	Europe
Contact	Patrick Corman	Janet Peng	Simon Loe
	Corman Communications, LLC	Spirent Communications	Spirent Communications
Direct Tel	+1-650-326-9648 +1-650-465-5973 (mobile)	+86 (10) 82330055 x160	+44 7850205885
E-mail	patrick@cormancom.com	janet.peng@spirent.com	Simon.Loe@spirent.com