SYNOPSYS®

ホワイトペーパー

ファジングによる 5G と IoT のセキュリティ対策

無線通信の普及

私たちのまわりはスマートフォン、Wi-Fi 対応ノート PC、Bluetooth ヘッドセットなどの無線通信機器からの電子信号であふれています。そのおかげで、私たちは外出先で電話、ショート・メッセージ、電子メールを利用したり、動画を観たりするなど、さまざまなタスクを実行できるようになっています。そして 21 世紀も 20 年が過ぎつつある今、無線通信の世界は第 5 世代移動通信システム「5G」への移行により、大きな飛躍を遂げようとしています。しかし、ここに至るまでは長い道のりでした。簡単に振り返ってみましょう。

移動体通信技術

1980 年代に登場した初期の移動体通信は、現在のものとは違って非常に原始的なものでした。世界初のアナログ・セルラー方式での通話に使われた第 1 世代の携帯電話は、その形状と重さ（2 ポンド =0.91 kg）から「ブリック（レンガ）」の愛称で呼ばれました[1]。1990 年代の第 2 世代デジタル携帯電話では、通話以外にショート・メッセージ・サービス（SMS）と呼ばれるテキスト・メッセージの送受信もサポートされました[2]。2000 年代初めには、WAP（Wireless Application Protocol）[3] をサポートした第 3 世代（3G）携帯電話が流行の最先端となり、モバイル Web サーフィンの原形が生まれました[4]。iPhone および Android スマートフォンが登場する 2007 ～ 2008 年頃には[5]、第 4 世代（4G）移動体通信によってモバイル機器でも十分な速度とスループットを備えた完全なブロードバンドが利用できるようになりました[6]。そして現在、4G の 1/10 の遅延と数百倍の容量を実現する 5G によって、移動体通信の性能はさらなる飛躍を遂げようとしています[7]。

IEEE 802.11：継続的な進化、そして 5G との連携へ

この時期に進化を遂げた無線通信技術は、移動体通信だけではありません。1997 年には、IEEE（Institute of Electrical and Electronics Engineers）LAN/MAN 標準化委員会（IEEE 802）が無線 LAN 向けプロトコル 802.11 を標準化し[8]、近距離の無線通信技術である Wi-Fi（Wireless Fidelity）が登場しました。この 802.11 プロトコルは屋内無線通信の基盤として、後のスマートフォン革命を支えることになります。しかし最初の 802.11 は最大スループットが 2 Mbps と低く、通信距離も限られていたため、それほど大きな成功には至りませんでした。

その後、802.11b を経て 2003 年に 802.11g が登場し、スループットは最大 54 Mbps、通信距離は 50 m 程度まで引き上げられました[9]。Wi-Fi 対応のコンピューターが次々と発売され、その数は 2006 年までに、爆発的な普及に必要とされる 1,000 万台に達すると予測されました[10]。以来、Wi-Fi による無線通信は職場や家庭、コーヒーショップ、空港をはじめ、自動車やバス、列車、飛行機での移動中など、あらゆる場所で利用できるようになり、その用途もほぼ無限に広がっています。2015 年以降も Wi-Fi に関しては Wi-Fi Calling などさまざまな技術革新が進むなど[11]、新しいタイプの機器やアプリケーションの登場に合わせて無線通信は着実に成長し、利便性の向上が続いています。

Wi-Fi は新しい規格が出るたびに通信距離、速度、スループットが向上しており、2019 年には理論上の最大転送速度 10 Gbps を達成した最新の Wi-Fi 6（IEEE 802.11ax）がリリースされています[12]。

このように移動体通信および Wi-Fi 技術はこれまで多くの進歩を遂げてきましたが、本格的な無線通信時代の幕開けはこれからです。今後は、5G と Wi-Fi の両方を活用した新しい技術が次々と登場するでしょう。特に IoT（Internet of Things）では、M2M（Machine-to-Machine）通信をはじめスマート・グリッド、乗用車やトラック、家庭用ドアフォン、あるいは衣服などへのセンサーの内蔵により、無線通信の爆発的な拡大が始まっています[13]。

第 5 世代（5G）移動通信システム

4G や LTE の最大 100 倍の速度、100 倍の容量、そして 1/10 の遅延を実現した 5G は、多くの産業に革命を起こすでしょう。5G のダウンロード速度は、4G の約 600 倍に相当する 10 Gbps に達します[14]。注意が必要なのは、5G は単一の技術ではなく、いくつもの先進技術の集合体であるということです[15]。5G の高い性能を実現するには、MIMO（Multiple Input Multiple Output）アンテナなどの新しい技術や、ミリ波などの新しい周波数帯を使用する必要があります。この新しい周波数帯を使用するには多くの無線アクセス・ポイントが必要で、一部には煙検知器と同程度の小型化が図られたものも存在します[16]。また、郊外での 5G 接続には、現在 3G および初期の 4G ネットワークで使用している周波数帯を転用することが必要となります。

性能の向上以外で 5G の最大の利点となるのが、4G や LTE に比べはるかに多くの機器にサービスを提供できることです。例えば Ericsson の予測では、インターネットに接続される IoT 機器の数は 2023 年末までに 200 億台を超え、これらはいずれも 5G を使用してインターネットに接続します[17]。

5G と「Wi-Fi 5G」

このように 5G が注目を集める中、ネットワークの種類が多いこともあって、「5G」の意味に関してやや混乱が生じています。ここで少し整理しておきましょう。セルラー 5G の「G」は「Generation（世代）」を表します。これに対し、いわゆる Wi-Fi 5G の「G」は「GHz」を表し、Wi-Fi が使用する周波数帯が 5GHz 帯であることを意味しています。つまり、どちらの名称にも「5G」が付いていますが、これらはまったくの別物です[18]。

名前はさておき、移動体通信の 5G が今後の主流になるのは間違いないでしょう。2023 年には世界の携帯電話出荷台数に占める 5G 対応機種の割合が 50% に達するとの予測が報告されています[19]。また、2020 年末までにほぼ 2/3 の企業が 5G を導入するとの予測もあります[20]。そして、5G を導入する企業の 59% が IoT 機器にも 5G を利用することを計画しています。IoT 機器は多くの企業が重要視しており、5G なら 1 平方キロメートル当たり最大 1,000 個のセンサー内蔵 IoT 機器をサポートできます[21]。

IoT およびコネクテッド・アプリケーションの現状と今後

未来の移動体通信技術の要となる 5G により、非常に多くの IoT 機器やコネクテッド・アプリケーションが実現します。これらは、既に実用化されたものもあれば、まだ概念段階のものもあります。

スマート・ホームの IoT 機器を 5G に接続したアプリから操作すると、照明の点灯・消灯やドアロックの解錠・施錠、さらには衣類乾燥機の停止などを実行できるようにもなっています[22]。Apple Watch や Fitbit などのウエアラブル機器も、5G を利用すれば追跡した健康データをほぼリアルタイムにアプリに送ることができます[23]。次世代のスマート・シティでは、信号機や大気モニターに 5G 対応の IoT 機能を持たせることにより、交通渋滞の緩和や、工場の操業停止による大気汚染の抑制などが可能になります。また、駐車スペースに空きができると通知したり、需要ピーク時の駐車料金を調整したりするスマート・パーキング・メーターは既に実用化されています[24]。最近は自動車内で Wi-Fi を利用できる「コネクテッド・カー」も登場していますが、5G の帯域幅を利用すれば車内にある機器を最大 10 台まで同時にネットワーク接続できます[25]。

セキュリティ課題の現状と今後

次世代ネットワークの 5G では性能が大きく向上する一方、5G を利用するアプリケーションや IoT 機器のアタック・サーフェスが拡大するという面もあります。既知のエクスプロイトだけでなく、未知の攻撃を受けることにもなります。インターネットや公共ネットワークにおけるセキュリティ侵害や攻撃は非常に危険性が高く、これまで多大な損害をもたらしてきました。IoT に対する過去の攻撃としては、以下のインシデントがメディアで大きく報道されました。

- **Mirai ボットネットによる分散型サービス妨害（DDoS）攻撃（2016、2018 年）：**IoT 機器のパスワードはデフォルトから変更されることがほとんどありません。Mirai は、デフォルトのパスワードをそのまま使用している IP カメラやホーム・ルーターなどの各種 Linux ベースの IoT 機器を総当たり攻撃によって乗っ取り、これらの機器を利用して New York Times、Spotify、Reddit などの有名サイトを含む米国の多くのサイトを何時間もダウンさせました[26]。
- **NotPetya ランサムウェア攻撃（2017 年）：**PC、サーバー、ネットワーク接続型ストレージ機器を標的にしたランサムウェア攻撃が急速に拡大し[27]、企業の被害額は総計 100 億ドルに達しました。Merck、Maersk、FedEx の 3 社だけでも被害額は 10 億ドルを超えています。もちろん、当時 5G ネットワークは存在していませんでしたが、このような攻撃がいかに大きな被害をもたらすかをこの事例は物語っています[28]。

無線に関する脆弱性にはまだ実証実験の域を出ないものもありますが、これらが実際に悪用されると大きな混乱を引き起こす可能性があります。

4G/LTE のエクスプロイト

IMP4GT（IMPersonation Attacks in 4G NeTworks）は、携帯機器と基地局の相互認証および通信方法に存在する脆弱性を悪用します。この脆弱性を利用すると、攻撃者は基地局を偽装したり、携帯電話のユーザーや機器に対してなりすまし攻撃を実行したりできます。これにより、有料サービスに勝手に申し込まれたり、誤った位置情報を送信されたりして正規ユーザーが法的責任を問われる可能性もあります[29]。

4G や LTE で攻撃者がネットワーク・スニファー（偽の基地局）を設置して中間者攻撃（MitM）を実行すると、30 万平方メートルを超えるエリア内にある接続機器の情報を取得できます。攻撃者は、これらの機器が Android か、iOS か、IoT 機器かを特定できます。そして、セキュリティが有効になる前の段階でこれらの機器にあるデータや設定を書き換えることにより、ハンドオーバーやローミングを妨害し、バッテリーを消耗させることができます[30]。

Wi-Fi のエクスプロイト

ネットワーク・セキュリティ・プロトコルの WPA2（Wi-Fi Protected Access II）は 15 年以上前から使われていますが、任意の機器が同じ Wi-Fi ネットワークに接続している他の機器の通信を横取りできるというセキュリティ上の問題が報告されています。WPA2 に見つかったゼロデイ脆弱性は、Wi-Fi ネットワーク・トラフィックの盗聴を可能にする KRACK（Key Reinstallation Attack）などいくつかあります[31]。幸い、WPA2 プロトコルおよび TLS 認証に関するファジング用のテスト・スイートが存在します。

WPA2 に代わるものとして、標準化団体 Wi-Fi Alliance は 2018 年にセキュリティを強化した新しいセキュリティ・プロトコル WPA3（Wi-Fi Protected Access 3）をリリースしました[32]。しかしセキュリティ規格やプロトコルは改良版を出してもすぐに新しい未知の攻撃が現れます。事実、WPA3 も WPA2 を置き換えた直後に Dragonblood 脆弱性が見つかっています[33]。

IoT のエクスプロイト

IoT には既知か未知かを問わず非常に多くの脆弱性があり、これらは医療機器のセキュリティと安全性に深刻な影響をもたらすことがあります。例えば、最近発見された Bluetooth Low Energy（LE）プロトコルの SweynTooth 脆弱性は、影響を受ける Bluetooth 機器の数が 2020 年 3 月の時点で 480 機種を超えています[34]。SweynTooth 脆弱性の例としては、スタックが予期しない公開鍵を受信した場合に発生する「Unexpected Public Key Crash」や、ATT 要求パケットを送信した後、応答を待たずに次の ATT 要求パケットを連続して送信するとデバイスが処理に失敗する「Sequential ATT Deadlock」などがあります。

2022 年にはネットワークに接続する IoT 機器の数が 146 億台に達するとも予測されており、攻撃者にとって標的は豊富に存在します。しかもこれら機器の多くを占める産業制御システムは元々インターネットに接続することを想定していなかったため、ネットワーク・スキャンのような単純な攻撃でさえ工場全体をダウンに追い込んでしまうことが危惧されます[35]。

ファジング・テストが必要とされる理由

ファジング・テスト（ファジング）は、LTE ネットワークに不正な形式の入力を与えてテストし、保護されていない初期プロシージャ、細工された平文のリクエスト、整合性保護が無効なメッセージ、セキュリティ・プロシージャのバイパスなどが正しく処理されているかどうかを調べます。これらの処理が正しく行われていないと、正当なユーザーに対する LTE サービスの妨害、SMS メッセージのスプーフィング、ユーザー・データ・トラフィックの盗聴や改ざんなど、さまざまな問題が発生する可能性があります。

次世代 5G では、SDN（Software-Defined Networking）やハイパーバイザー、ネットワーク・スライシングなどの仮想化技術を利用して膨大なアプリケーションおよびワークロードをネットワーク・エッジ上で実行、管理、およびスケーリングすることになり、5G のユース・ケースを予測して構成するのは今以上に困難になります。また、こうした新しい未知のベクターによって表面化する潜在的なセキュリティ・リスクを緩和することも難しくなります。

ファジング・テストは、新しい未知のバグや脆弱性、そして重大な影響を与えかねないクラッシュの発見に役立ち、防御の第一線、および最後の砦の役割を果たします。

ファジングの仕組み

ファジングでは、ネットワークに接続した機器に不正な形式のデータを送信し、エラー、欠陥、システム・フリーズ、弱点を顕在化させます[36]。ファジング・テストは、意図的に不正な形式の入力（テスト・ケース）をソフトウェアに送信し、エラーが発生するかどうかを見ます。エラーが発生した場合はバグが発見されたことになり、これを修正することによってテスト対象のソフトウェアの堅牢性とセキュリティが改善されます。

対象となるソフトウェアをテストするプログラムのことを「ファザー」と呼びます。ファザーに求められる条件としては、記録を残す機能があること、対策に役立つ具体的なレポートが生成されること、そしてエラーを再現できる円滑な修正プロセスによって不具合を確実に修正できることが挙げられます。

ファジングは、まだその存在も回避策も知られていないようなゼロデイ脆弱性を特定する手法として大きな効果があります。ファザーにはいくつかの種類があります。どのファザーが最適かは、テストの目標をどこに置くかによって異なります。ファジングの種類の詳細は、シノプシスのホワイトペーパー「What Is Fuzzing: The Poet, the Courier, and the Oracle」を参照してください。

先進世代のファジング・ツール「Defensics」

Defensics は、大企業などソフトウェア・システムにおけるセキュリティの弱点を効果的かつ効率的に見つけて修正したいというニーズに幅広く応える先進世代のファザー（ファジング・ツール）です。Defensics では、体系的かつインテリジェントなアプローチでネガティブ・テスト（異常系テスト）を実行できるため、企業は製品のイノベーションやタイム・トゥ・マーケット、運用コストを一切犠牲にすることなく、ソフトウェアのセキュリティ対策をとることができます。Defensics を使用すれば、5G にもセキュリティを組み込むことができます。例えば、最近追加されたテスト・スイートを使用すると、5G 基地局とユーザー機器の間のコントロール・プレーン（C-Plane）信号を Defensics でテストできます。

Defensics は他の種類のファジング・ツールより多い既製の生成テスト・スイートを 300 個近く用意しています。このため、ユーザーは面倒なマニュアル・テストを作成する必要がなく、すぐにファジングを実行できます。シノプシスは、Defensics のテスト・スイートを継続的に更新しており、最新のテクノロジーをサポートできるように新しい入力型、仕様、RFC（Request for Comments）への対応を進めています。

次世代の核となる移動体通信と IoT 技術をサポート

ネットワーク機器メーカーとサービス・プロバイダーのほとんどが 5G への投資を開始しています。また、特に NSA（非スタンドアロン）モードの 5G では、LTE eNodeB（eNB）基地局とアンカー接続し[37]、一部の動作を LTE ネットワークに切り替えて実行する必要があるため[38]、現行世代の移動体通信インフラストラクチャの基盤となっている 3G/4G プロトコルが 5G でも使用されます。これを図 1 に示します。

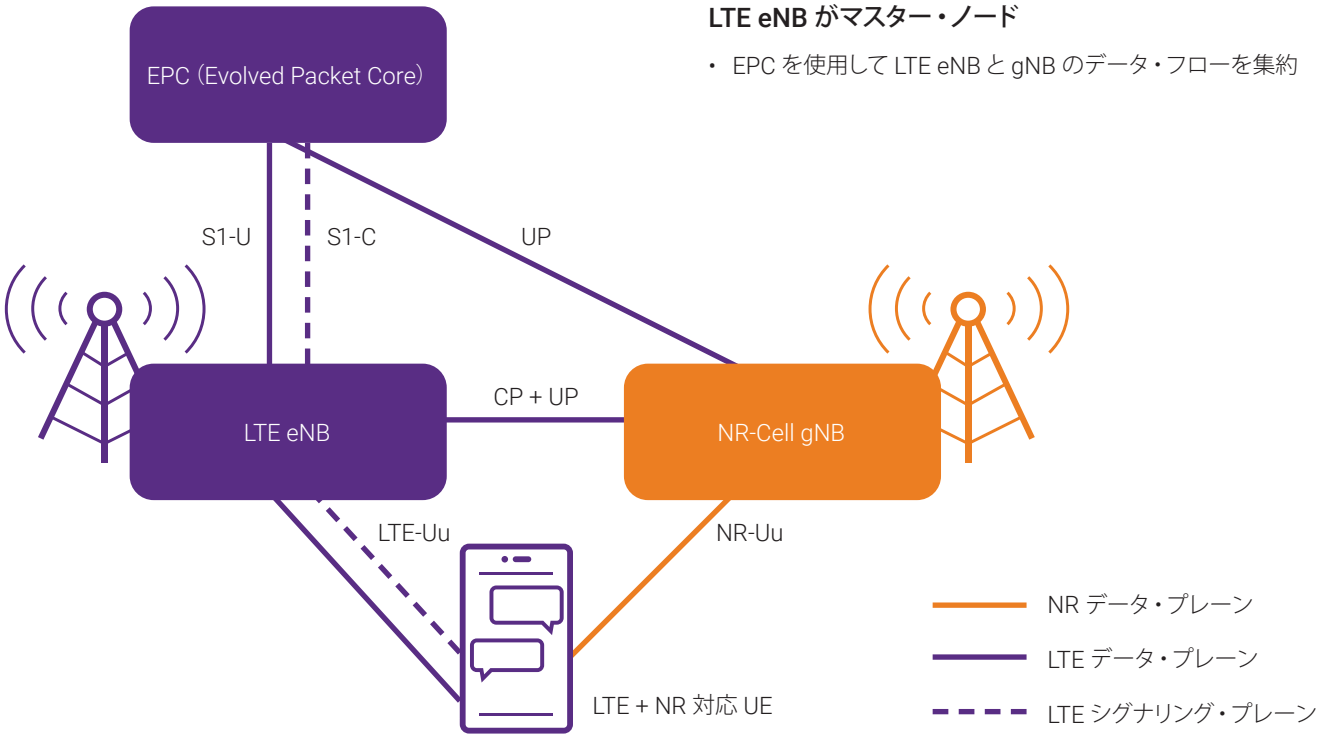

図 1：マスター・ノードとしての LTE eNB

4G や LTE および 5G の移動体通信以外にも、Defensics のテスト・スイートは Wi-Fi や Bluetooth などの無線を幅広くサポートしており、移動体通信コア、ネットワーク、IoT、メディア通信など多岐にわたるテストを容易に実行できます。

IoT 機器と現代のインターネット

IoT 機器は、現代のインターネットの重要な一角を占めています。これらはさまざまなプロトコルを利用してインターネットに接続し、医療機器など重要な用途で使われています。しかしこれら機器の動作を脅かすものとして、最近 Bluetooth Low Energy (LE) に SweynTooth と呼ばれる一連の脆弱性が見つかっています[39]。

こうした IoT 機器のセキュリティも、Defensics と Bluetooth LE テスト・スイート・パッケージを組み合わせればチェックが可能です。例えば、Bluetooth LE SMP Client テスト・スイートを使用すると、予期しない公開鍵を送信して IoT 機器がクラッシュする脆弱性があるかどうかをテストできます。また、Bluetooth LE ATT Server および ATT Client テスト・スイートを使用すると、ATT 応答を待たずに ATT 要求パケットを繰り返し送信した場合に IoT 機器がフリーズする (デッドロック状態になる) かどうかをテストできます。

また、Defensics には MQTT Client、MQTT Server、IPv4、802.11 WLAN などの各種 IoT 機器向けテスト・スイートも用意されており、これらを使用して IoT 機器をチェックし、さまざまな種類のサービス妨害 (DoS) 攻撃を未然に防ぐことができます。

IoT 機器は、ボットネットの標的にもなることが明らかになっています。これは、IoT 機器の多くが一般的な Linux オペレーティング・システムを使用しており、これら OS のカーネルに脆弱性があるためです。しかし近年、ファジング・テストによってこうしたセキュリティの欠陥が発見・修正されています。シノプシスの R&D チームは、Defensics と NFS3 Server テスト・スイートを使用して、このような Linux カーネルの脆弱性を 3 つ発見しました。実は 2014 年に、無数の企業と消費者に影響を与えた Heartbleed 暗号化脆弱性を発見したのも同じチームで、その時も Defensics が使われています。

4G/5G プロトコルおよびセルラー通信の脆弱性

5G ネットワークにおけるセルラー通信には、少なくとも 10 個以上の新しいプロトコルと、4G や LTE で使われていたプロトコルを 5G 向けに改良したものが 30 個ほど使用されます。例えば PFCP (Packet Forwarding Control Protocol) は 5G で導入されたパケット・プロトコルですが、4G/LTE でもコア・ネットワークの機能エレメントを接続して 4G および 5G サービスを提供するために使用されます。

その他の重要なプロトコルとして、ユーザー機器のシグナリングおよびモビリティ / セッション管理を実行する S1AP/NAS や NGAP/NAS などがあります。このようにアタック・サーフェスが拡大すると、新しい未知の脆弱性が必ず発生します。

PFCP Server、PFCP Client、S1AP/NAS Client、NGAP/NAS Client などの各種 Cellular Core テスト・スイートを使用して、Defensics は悪意のある基地局またはユーザー機器としてふるまい、テスト対象に対して例外的または異常な要求を送信します。

独自の開発ライフサイクルとカスタム・プロトコルへの対応

慣習にとらわれない独自の開発ライフサイクルを導入している企業にも、経験豊富なシノプシスのプロフェッショナル・サービス・チームがファジング・テストのチェックポイント特定とメトリクス定義、およびファジング・テスト・マチュリティ・プログラムの作成を支援します。

また、独自のカスタム・プロトコルやインターフェイスのセキュリティ対策が必要な場合は、Defensics ファジング・テスト・ソフトウェア開発キット（Defensics SDK）を使用することで、エクスプロイトを未然に防ぐことができます。この SDK が提供するファジング・フレームワークにより、一般的でない独自のカスタム・プロトコルに対して専用のテスト・スイートを開発できます。

まとめ

アプリケーション、社会、国家が 5G でつながる未来はすぐそこに迫っており、これによって電気通信、産業制御、ゲーム、遠隔医療など多くの産業に革命が起こることが期待されています。速度とスループットの向上、および遅延の低減により、インターネットを介した仮想現実（VR）や拡張現実（AR）など、これまでなかなか実現しなかったアプリケーションがいよいよ現実のものとなります。

しかし、こうした機能の向上に伴い、SDN インフラストラクチャやエコシステムは複雑さを増し、アタック・サーフェスの拡大を招いているほか、産業用制御システム（ICS）のように元々インターネットへの接続を想定していなかったレガシー・ネットワークにも 5G が統合されるようになっています。これらのレガシー・ネットワークにはセキュリティの欠陥が数多く潜んでおり、5G およびエッジ・コンピューティングに完全に移行して IoT がより普遍的なものになれば、新しい攻撃にさらされる危険があります。

このようなセキュリティ・リスクの高まりを考えると、次世代 5G ネットワークは政府や企業にとって、より堅牢な品質およびセキュリティのフレームワークを新たに確立する好機であるとも言えます。こうしたリスクに対処すべく、NIST（米国標準技術研究所）や 3GPP などの機関はサイバーセキュリティ・フレームワークを発表しており、これらを業界にとってのベスト・プラクティス・ガイドとして利用することも可能です。

5G と IoT 機器およびアプリケーションに対するファジング・テストの詳しい実行方法は、Defensics の Web ページを参照してください。

参考文献

1. GCN, How Much Did the First Handheld Cell Phone Weigh?, Sep. 22, 2011.
2. Techopedia, Short Message Service (SMS), May 28, 2019.
3. Chris Bennett, Wireless Application Protocol 2.0, InformIT, Nov. 9, 2001.
4. NTE, What Is WAP Mobile Web, LoveToKnow, accessed June 29, 2020.
5. Robin Parrish, Which Came First: iPhone or Android?, Apple Gazette, May 3, 2012.
6. Aditi Chakraborty, A Study on Third Generation Mobile Technology (3G) and Comparison Among All Generations of Mobile Communication, International Journal of Innovative Technology & Adaptive Management 1, no. 2 (November 2013).
7. Rahul Gupta, 6 Interesting 5G Wireless Technology Features That Make it Superior to 4G/3G, Guiding Tech, April 4, 2018.
8. CableFree, The History of WiFi: 1971 to Today, May 18, 2017.
9. C. Suresh, V. Vidhya, et al., Wireless Fidelity, International Journal of Research in Computer Applications and Robotics 4, no. 2 (February 2016), pp. 50–59.
10. The Economist, A Brief History of Wi-Fi, June 12, 2004.
11. Chris Neiger, Is Wi-Fi Calling the Future of Wireless?, The Motley Fool, July 12, 2015.
12. Brandon Conroy, What Are the Real Benefits of Wi-Fi 6—Everything You Need to Know, Windows Dispatch, March 8, 2020.
13. Ahlem Saddoud, Wael Doghri, et al., 5G Radio Resource Management Approach for Multi-Traffic IoT Communications, Computer Networks 166 (Jan. 15, 2020).
14. Finley, The WIRED Guide to 5G.
15. Klint Finley, The WIRED Guide to 5G, Wired, Dec. 18, 2019.
16. Wikipedia, Extremely High Frequency, updated June 22, 2020.
17. IoT Business News, Ericsson Forecasts 20 Billion Connected IoT Devices by 2023, Dec. 8, 2017.
18. Colin Berkshire, The Difference Between 5G and 5G, TalkingPointz, April 24, 2019.
19. Rae Hodge, A 5G Phone Boom Is Coming, but Maybe Not Until 2022, CNET, Jan. 22, 2020.
20. Gartner, Gartner Survey Reveals Two-Thirds of Organizations Intend to Deploy 5G by 2020, Dec. 18, 2020.
21. Ibid.
22. Rajesh Mishra, 15 Examples of Internet of Things Technology in Use Today, Beebom, Jan. 31, 2020.
23. Andrew Meola, A Look at Examples of IoT Devices and Their Business Applications in 2020, Business Insider, Dec. 18, 2019.
24. Ibid.
25. AT&T, Connected Car From AT&T—Unlimited Data for Your Car, accessed June 29, 2020.
26. Josh Fruhlinger, The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet, CSO, March 9, 2018.
27. Iain Thomas, Everything You Need to Know About the Petya, er, NotPetya Nasty Trashing PCs Worldwide, The Register, June 28, 2017.
28. Tom Wheeler and David Simpson, Why 5G Requires New Approaches to Cybersecurity, Brookings, Sept. 3, 2019.
29. Ravie Lakshmanan, New LTE Network Flaw Could Let Attackers Impersonate 4G Mobile Users, The Hacker News, Feb. 26, 2020.
30. Karen Epper Hoffman, 5G Inherits Some 4G Vulnerabilities, GCN, Oct. 21, 2019.
31. Charlie Osborne and Zack Whittaker, Here's Every Patch for KRACK Wi-Vi Vulnerability Available Right Now, ZDNet, Oct. 17, 2017.
32. Mohit Kumar, Wi-Fi Alliance Launches WPA3 Protocol With New Security Features, The Hacker News, Jan. 9, 2018.
33. Catalin Cimpanu, Dragonblood Vulnerabilities Disclosed in WiFi WPA3 Standard, ZDNet, April 10, 2019.
34. NetSec.News, More Than 480 Bluetooth Devices Affected by SweynTooth Vulnerabilities, March 5, 2020.
35. Ben Heubl, How to Hack an IoT Device, E&T, June 10, 2019.
36. Techopedia, Fuzz Testing, accessed June 29, 2020.
37. AT&T, 5G Update, accessed June 29, 2020.
38. Telecompaper, 3GPP Approves First 5G Standards, Dec. 21, 2017.
39. U.S. FDA, SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication, March 3, 2020.

SYNOPSYS®

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質なソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や不具合を迅速に見つけて修正します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社
ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software