レポート

McAfee
Together is power.

McAfee Labs 2018 年の脅威予測
～来年のサイバーセキュリティ動向 5 項目を展望

McAfee Labs 2018 年の脅威予測 ～来年のサイバーセキュリティ動向 5 項目を展望

※ 本レポートは、2017 年 11 月 29 日更新の McAfee Blog の内容です。McAfee Labs と Office of the CTO のメンバーが作成したものです。

McAfee Labs の 2018 年脅威予測レポートをご覧いただきありがとうございます。現在のサイバーセキュリティをめぐる状況は、日々、新しいデバイス、リスク、脅威が生まれ、激しく変化しています。今回のブログでは、McAfee Labs と Office of the CTO に所属する多くの専門家に意識調査を行いました。機械学習、ランサムウェア、サーバーレス アプリ、またプライバシーの問題など、脅威に関する幅広い見解を得ることができました。

防御者と攻撃者の間で機械学習を活用したサイバーセキュリティ ツールの“ 開発競争”が激化

新たなサイバー攻撃の急増やその被害の大きさから、すぐにそれらの脅威を検知できる対策が求められており、重要なセキュリティ ツールとしての機械学習にますます注目が集まっています。しかし残念ながら、機械は仕事の相手を選ばないので、防御側と攻撃側の間で機械学習を活用したサイバーセキュリティ ツールの“開発競争”が激化しています。人とテクノロジーのコラボレーションには、防御者が優位に立てる大きな可能性が秘められており、それを実際に現実のものとすることが、今後数年間の私たちの使命です。テクノロジーを使った検知や復旧のモデルの崩壊を防ぐだけでなく、敵が攻撃を強化するよりも速く防御能力を進化させる必要があるでしょう。

サーバーレス アプリが攻撃側にも防御側にも新たな機会をもたらす

サーバーレス アプリにより、ユーザーは時間とコストを削減できますが、一方で権限昇格攻撃、アプリケーション同士の相互依存性を悪用した攻撃、ネットワーク内を移動するデータへの攻撃などの脆弱性が発生するため、ブルートフォース攻撃／ DoS 攻撃を増加させます。サーバーレス アプリにより、速やかなサービス料金の支払いなど、細かい対応が可能になりますが、権限昇格攻撃やアプリケーションの依存性を悪用した攻撃には脆弱です。また、サーバーレス アプリでは、複数サーバーに機能を実行するために必要なデータが分散していることもあるため、それらのサーバー間をつなぐネットワークを移動中のデータを狙う攻撃も受けやくなります。機能開発や導入には適切なセキュリティ対策を実施し、トラフィックは VPN や暗号化で適切に保護する必要があります。

目 次

企業が家庭内のプライバシー情報を血眼になって収集

家庭内で使われるコネクテッド デバイスの増加に伴い、企業側は、おそらくユーザーが不快に感じるレベルまで、その挙動を観察し、ユーザーのプライバシーについて把握しようとする可能性があります。マカフィーでは、企業はこうした家庭のデータをより多く取得するための新しい方法を模索するようになると予想しています。企業は必要経費としての罰金を支払うことも視野に入れながら、製品やサービスの利用規約を変えてでもより多くの個人情報を取得しようと試みるでしょう。ユーザーがこのような問題から身を守ることは一層難しくなり、来年以降は企業による個人情報に関する違反や違法行為の検挙数が大幅に増えると予想しています。

子供が抱えるデータというお荷物

この変化する世界で最も危険にさらされているのは、おそらく子供たちでしょう。子供たちは、将来的に素晴らしいガジェット、サービス、体験を得ることができますが、とてつもなく大きなプライバシーのリスクにもさらされています。子供たちが未来のデジタル世界を存分に楽しめるようにするためには、抱えているデータという荷物の整理整頓の方法を教える必要があります。この世界からプライバシーが大きく消えつつあります。多くの人々がこの状況に問題を感じていないようですが、インターネット上で行われた分別のないコンテンツ投稿や思慮の足りない行為が、将来的に人生を変える結果を招くことになるかもしれません。

防御者と攻撃者の間で機械学習を活用したサイバーセキュリティ ツールの“ 開発競争”が激化

攻撃側も防御側も、相手より優れた革新的な AI 技術を実現するために戦いを繰り広げる

人とテクノロジーのコラボレーションは、サイバーセキュリティに欠かせない要素となっています。テクノロジーが実現するスピードとパターン認識で、人間の判断や意思決定を強化します。脆弱性の検知と復旧、不審なふるまいの特定、ゼロデイ攻撃の封じ込めなど、すでに幅広いセキュリティ分野で機械学習が取り入れられています。

2018 年は、その開発競争の激化を予想しています。敵は、機械学習を使って攻撃を開発したり、人工知能（AI）も含めて色々な攻撃法を試すことで、防御側の機械学習モデルを把握し、その妨害活動を拡大させるでしょう。研究者は、来年度中に攻撃のリバース エンジニアリングを行い、何らかの機械学習が利用されていることを証明するものと予想しています。すでに、脆弱性を探し、過去のモデルとは異なる検知されにくい方法で攻めてくるブラックボックス型の攻撃が確認されています。攻撃者は、こうしたツールをどんどん取り入れ、それらの各種ツールと攻撃手法を斬新な方法で融合させるでしょう。機械学習を使って、人間では不可能な量のデータを採取･統合し、ソーシャル エンジニアリング力を強化してくるかもしれません（その結果として、フィッシング攻撃の検知が一層難しくなります）。増加するコネクテッド デバイス上の脆弱な認証情報やデバイスから盗まれた情報を悪用した攻撃が大きな効果を上げるかもしれません。あるいは、脆弱性スキャンを行い、発見した脆弱性を悪用するまでの時間を短縮することで、攻撃スピードを上げてくるかもしれません。

防御側が何か新しいものを取り入れると、必ず、攻撃側もそれについてできる限りの情報を把握しようとします。敵は、マルウェアのシグネチャやレピュテーション システムなどで、何年も前からそうした行為を行っているため、機械学習モデルでも同じことが起こると予想しています。たとえば、外部から探索してモデルをマッピングする、公表された調査内容や公共の資料を検討する、また内通者を利用しようとするなどの行為が行われるでしょう。その目的は、防御の回避や妨害です。攻撃者は、目の前のモデルを再現した後に、そのモデルを回避したり妨害したりしてマルウェアを侵入させるか、何も侵入させずにモデルを無価値なものにするでしょう。

防御側も、機械学習、AI、ゲーム理論を組み合わせて、保護すべきソフトウェアやシステムに潜む脆弱性を探し、犯罪者に利用される前に、そうした弱点を修正しようとするでしょう。これは、テクノロジーの膨大な能力と独自の洞察に基づきバグやその他の不正利用可能な脆弱性を探すといった侵入テストの次のステップと考えてください。

防御モデルを狙う攻撃に対抗するため、防御者はエンドポイント、クラウド、データ センターに、それぞれ独立して稼働する防御モデルを導入するようになるでしょう。各モデルは異なる入力データやデータ セットで検証されるため、多層的な保護を実現できます。データに関して言うと、機械学習モデルの開発における最大の課題は、急激に変化するマルウェア環境を代表する適切なデータを収集することです。来年は、研究者がデータ セットの経験を積み、古いデータや不良データに関する知識を深めるに伴い、この分野が進歩し、検証方法や感度テストの向上につながると予想しています。

テクノロジーが台頭しています。テクノロジーは、データ、コネクティビティ、そして電源を与えてくれる人であれば、どんな人のためにも働きます。私たちの仕事は、攻撃者よりも早くテクノロジーを進化させ、防御モデルが解明

／妨害されないように保護することです。人とテクノロジーのコラボレーションにより、攻撃者に対する優位性を取り戻す可能性を高めることができます。

従来の脅迫型ランサムウェアの標的、テクノロジ、目的が変化する

ランサムウェアの標的、テクノロジー、戦術、ビジネスモデルが、従来型から新たなものへと変化

マカフィーは、2018 年以降も続くと予想しているランサムウェアの能力と手口が進化していることを確認しています。

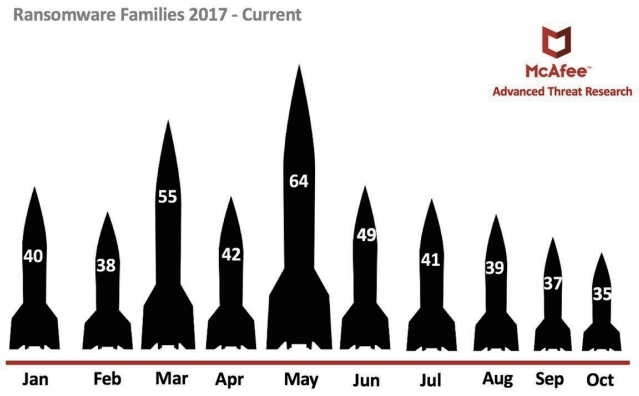
従来型のランサムウェアについては良いニュースがあります。McAfee Labs は、過去 1 年間でランサムウェアの合計数が 56% 増加したことを確認しましたが、McAfee Advanced Threat Research（ATR）チームが得た証拠から、同時期のランサムウェアに対する身代金支払額は減少していることが明らかとなりました。

マカフィーの研究者は、この傾向は、システム バックアップに対する意識の向上、無料の復号ツールの登場、ユーザーや組織の認知向上、マカフィーが参画する NoMoreRansom.org や Cyber Threat Alliance などの業界を挙げた対策により、過去 12 カ月間の防御成功率が上昇していることの表れであると断言しています。

サイバー犯罪者は、この状況にどう順応しているのでしょうか。このように防御成功率が上がっているため、攻撃者はランサムウェアの標的をより高額の身代金を支払える人物や、ベンダー、業界、教育による対策が不足している新規デバイスなどの高価値対象へと変更せざるを得なくなっています。

財産価値がより高い対象を狙う攻撃では、スピア フィッシング メールを介してランサムウェアを送り込めるソーシャル エンジニアリングの手法を巧みに利用して、特定の標的に狙いを定めた攻撃のパーソナライズ化がさらに進むでしょう。こうした高価値の標的は、最新のスマートフォンのような、高価になってきている個人用デバイスなどのエンドポイントで攻撃されるでしょう。これらのデバイスではクラウドにバックアップが作成されるため、比較的、従来型のランサムウェアの被害に遭うことはありません。そのため、攻撃者は身代金が支払われるまで携帯電話を「操作不能」にすることを企むようになると予想しています。

マカフィーは、ランサムウェアがこのように変化していることから、攻撃が高価値標的向けのテクノロジーや戦術に絞られ、攻撃者の技術が向上し、サービスとしてのランサムウェア プロバイダーの能力が向上・特殊化する傾向が進み、それがランサムウェア ファミリー総数のわずかな減少につながっていると考えています。



2017 年に発見された新たなランサムウェア ファミリー数。平均で 1 カ月あたりに新規発見されるサンプルの 20 ～ 30% が、Hidden Tear ランサムウェア コードをベースとしている。
出典 : McAfee Labs

精緻さに欠け、認知度が高く、容易に予想され得る 1

対多数型のテクノロジーや戦術、プロバイダーを使った攻撃からは、投資に見合った見返りを得ることはできません。

幅広く認知されているランサムウェア ファミリーが長期的に存続し、蔓延している場合、実績と信頼性に優れたランサムウェア サービス プロバイダーが背後にいるに違いありません。現在の Locky ファミリーがその好例です。

デジタル世界が実世界に影響を及ぼすことがあります。毎年、交通、水道、電気などの産業システムへのセキュリティ侵害が現実世界の安全性に与える脅威について予測されています。また、自動車からコーヒーメーカーに至るまで、消費者が利用する製品が大量にハッキングされることで物理的な脅威がもたらされるという想定のシナリオを毎年のように作って検討もしています。

マカフィーは、掃除機にも危険が潜んでいると警告するサイバーセキュリティ ベンダーの輪から一線を引きたいと考えています。しかし一方で、マカフィーの研究者は、デジタル攻撃が現実世界に影響を与えることを、実際に予想してもいます。サイバー犯罪者は、富裕層や企業向けに高額なサービスや機能を提供しているコネクテッド デバイスにランサムウェア攻撃を仕掛けることを目論んでいるからです。

山道を運転するおばあさんの車のブレーキ制御を掌握するよりも、企業の重役が乗る高級車にランサムウェア攻撃を仕掛けて出勤を邪魔する可能性のほうが高く、サイバー犯罪者にとって収益性も高いと、研究者は信じています。コーヒーメーカーを使って何百万軒もの家に火を点けるよりも、真冬に裕福な家庭のサーモスタットを攻撃する可能性のほうが高く、収益を得られる確率も高いはずです。

こうした方法を含め、サイバー犯罪者は致命的な損害ではなく、個人に物理的なダメージを与えるデジタル攻撃を開発する方が得だと考えるようになるはずです。

ランサムウェアは身代金の取得にとどまらず、妨害や破壊活動へと進化を見せています。WannaCry や NotPetya などのランサムウェアの発生は、ランサムウェアが従来の身代金目的ではなく、明らかなシステムの妨害や破壊を目的として、新しい方法を取り入れてくることを示しています。

WannaCry や NotPetya によるランサムウェア攻撃では、短期間で数多くのシステムが感染しましたが、被害に遭ったシステムを回復させるための決済機能や復号機能は設けられていませんでした。これらのランサムウェアの正確な目的は未だ不明ですが、マカフィーでは、膨大なコンピューターで構成されるネットワークに対するあからさまな妨害または破壊か、真の目的をくらますために行われた DDoS 攻撃と同じように、実際の攻撃から IT セキュリティ チームの目を逸らさせることが、攻撃者の目的だったのではないかと考えています。妨害力や破壊力を誇示したり、将来、企業向けに極めて大規模な脅迫行為を行うことを意図した壮大な概念実証であった可能性も考えられます。

2018 年、マカフィーは WannaCry や NotPetya に倣ったランサムウェアが確認されるであろうと予想しています。サービスとしてのランサムウェア プロバイダーは、NotPetya 攻撃者が世界中の企業でグローバル IT システムを機能不全に陥れたのと同じような方法で、国家的、政治的、そしてビジネス上のライバルを混乱させることを目論んでいる国家、企業、そして野望を持った人々に攻撃を売るようになるでしょう。競合企業による不正な行為であれ、みかじめ料を強要するマフィアを真似たサイバー犯罪者の仕業であれ、損害を与えることを目的とした攻撃は増加すると予想しています。

このランサムウェアの兵器化という考え方は、一見、ランサムウェアのテクノロジーや戦術的なコンセプトの定義を不必要に拡大させてしまうように思えるかもしれません。しかし、ワームのように急速に繁殖する能力と致命的な破壊力やダメージを備えているのに、それを止めるためにわざわざ身代金を要求する WannaCry や NotPetya にあなたの企業が感染した場合、果たしてこれらのランサムウェアの目的は何でしょうか。

当然、2017 年に発生したランサムウェアに対する最大かつ避けて通れない疑念が沸いてきます。WannaCry や NotPetya は、本当に莫大な収益を獲得し損ねたランサムウェア攻撃だったのでしょうか。それとも、大きな成功を収めた組織の殲滅作戦だったのでしょうか。

最後に、マカフィーは、こうしたランサムウェア攻撃の特性と目的の変化や、実際に致命的な金銭的損害が発生する可能性があることから、一連のランサムウェア関連保険を含むデジタル関連保険商品を拡販したい保険会社にとってのビジネスチャンスが生まれると予想しています。

サーバーレス アプリが攻撃側にも防御側にも新たな機会をもたらす

サーバーレス アプリはコンテナや仮想マシンと同等レベルのセキュリティを目指す

仮想コンピューティングの最新トレンドである“サーバーレス”アプリによって、より新しい次元の細やかなコンピューティング機能を実現できます。最近、一部のプロバイダーが料金請求サイクルを数秒以内にまで短縮しましたが、この機能は売上増加に大きく影響することが予想されます。料金の請求に数分から数時間を要するコンテナや仮想マシンを使用する代わりに、数秒以内で処理できるサーバーレス アプリを使うことで、一部の事業者はコストを 1/10 に削減できるでしょう。

しかし、このような機能を実行する際のセキュリティはどうなのでしょうか。権限昇格攻撃やアプリケーション同士の相互依存性を悪用した攻撃などの従来からの攻撃に対する脆弱性があるだけでなく、データが移動する際に攻撃を受けるリスクや攻撃対象の増加など、新たな脆弱性も潜んでいます。

従来型の脆弱性から見ていきましょう。急いで導入されたサーバーレス アプリは、不適切な権限レベルを使用し、その環境を権限昇格攻撃の危険にさらす可能性があります。同様に、急いで導入されるため、企業の管理下にない、適切に検証されていない外部のレポジトリから取得したパッケージに依存した機能になる可能性があります。

また、新たなリスクもあります。ユーザーは URL を見れば、サーバーレスの環境に送られるリクエストかどうかを判断できるため、攻撃者は外部からそのサーバーレスアプリを支えるインフラを妨害または無効にし、多数の組織に影響を与えることができるかもしれません。

機能を実行するために必要なデータにも危険が潜んでいます。アプリの実行に必要なデータが、機能を実行するサーバーと同じサーバー上にないこともあるため、何らかのネットワークを経由する必要があった場合に、データの傍受や不正操作のリスクにさらされるかもしれません。

マカフィーは、サーバーレス アプリでサービスの粒度が増すことで、攻撃対象が大幅に増えると予想しています。複数のプロバイダーを経由する機能が増えるということは、攻撃者が悪用ないしは妨害できる領域が増えることを意味しています。サーバーレス アプリの機能の開発や導入プロセスには、必ず必要なセキュリティを含め、VPN や暗号化でそのトラフィックを適切に保護してください。

企業が家庭内のプライバシー情報を血眼になって収集

制御しなければ、ユーザーのプライバシーは企業の手に渡ってしまうかもしれない

企業には、コネクテッド ホーム機器の所有者の購入ニーズや嗜好を観察し把握したいという強い動機があります。大抵のユーザーが知らないところで、すでにネットワークに接続されたデバイスから膨大なデータが送られています。ユーザーは滅多にプライバシー ポリシーを読まず、そのことを知っている企業はデバイスやサービスが購入された後に頻繁にポリシーを変更し、より多くの情報を収集して追加の売上機会を得ようと考える可能性があります。

2018 年、コネクテッド ホーム機器のメーカーやサービス提供企業は、ユーザーの個人的なデータを収集することで（ユーザーとの合意の有無にかかわらず）、実質的にユーザーの家庭を企業の製品やサービスのお得意先に仕立て上げ、一個一個の製品では少ない営業利益を数で稼ごうとするでしょう。

このような企業側の意識が働いているだけでなく、デバイス メーカーも技術的にこれを実現することが可能であるため、企業はデバイスやサービスを割引する代わりに、ユーザーのふるまいを極めて個人的なレベルまでモニタリングできるようにするかもしれません。

部屋、デバイス、アプリに家電の状態をモニターし、パートナー企業に送信するためのセンサーや制御機能を搭載することは簡単で、消費者に特別アップグレードや機種変更を打診するだけです。

すでに子供の玩具は、子供のふるまいをモニタリングし、ブランドのコンテンツ購読やオンライン教育プログラムのアップグレードを含め、新しい玩具やゲームを提案できるようになっています。

自動車メーカーやサービス センターも、特定の車両の場所を把握し、所有者の予定表やパーソナル アシスタントと調整して、通勤計画を管理・支援することができます。所有者の好みや頻繁に利用している飲食店からのスペシャル オファーに基づき、コーヒーショップやスーパーマーケットなどの店舗への立ち寄りを自動的にスケジュールに組み込むことが可能です。

これが消費者のユートピアなのか、企業のユートピアなのか、あるいはプライバシー擁護論者にとっての悲惨な悪夢なのかはわかりませんが、こうしたシナリオの多くが現実になろうとしています。

現在、さまざまなデバイスやサービスから収集したデータの利用方法は、大抵の人が考えるよりも遥か先を行っています。

もちろん、ユーザーはデータが収集されることに法的に同意しているのですが、企業側のこうした行為を認識している技術的知識が豊富な人たちでさえ、利用規約を読まずに同意しているため、後から規約を変更し、規約にないことまで行う企業も出てくるかもしれません。

近年、企業の違反行為を数多く発生しています。ある懐中電灯アプリを開発する企業のライセンス契約には、アプリが地理位置データを収集することが記載されていませんでした。3 年前、あるビデオ ゲームのハードウェア企業が、拒否できないアップデートをプッシュしたことがありました。つまり、ユーザーは新しい規約に同意しなければ、購入した製品を使用できなくなるのです。多くの利用規約で、ユーザーは企業が一方的に行うあらゆる将来的な変更事項にも「同意」しています（「変更後にサービスの使用を続行した場合、ユーザーはこの変更に同意したと解釈されるものとします」）。

7月、米国連邦捜査局（FBI）が、インターネットに接続される子供の玩具から子供の個人情報を収集できる可能性があるとして保護者に警告を出しました。

企業側は、今後も家庭というプライバシー空間の中で、ユーザーが何を、どのように使用しているかを把握しようとし、ユーザーが共有したくないデータまで要求するようになることは間違いないでしょう。マカフィーは、かなりの数の企業が個人情報を保護する法律に違反することで、追加の販売機会の創出など大きな利益を得ることができるため、違法と知りつつその対価として罰金を払い、より多くの個人情報の収集を続けるようになると断言します。ですが、先日、FBI が玩具について保護者に警告したことから、このようなアプローチには、規制や刑事上の法的責任を問われるようになるかもしれません。

来年は、企業がコネクテッド ホームの可能性を上手く活用しているケースや、これを悪用したケースをさらに確認することができると思います。

本記事の作成にご協力いただいた電子フロンティア財団（Electronic Frontier Foundation ：EFF）に感謝の意を表します。

子供が抱えるデータというお荷物

企業によるユーザー生成コンテンツの乱用から子供を守る

好むと好まざるとにかかわらず、現在、私たちが利用しているすべての製品、サービス、体験から、何らかのデジタル記録が生成されています。そのため、大人は徐々にこの状況に折り合いをつけ、自らのデジタル生活を管理することを学んでいきます。一方、子供たちはどうでしょうか。企業の人材の採用判断は、すでにインターネット検索の結果に影響されています。これが学校、医療、行政にまで広がれば、どうなるでしょうか。子供たちは、長時間動画を見たことが原因で、学校への入学を拒否されるのでしょうか。あるいは、7 歳の時に作った動画が原因で、公職選挙に立候補できなくなるのでしょうか。

インターネット上の情報は、プラスにもマイナスにも働く可能性があります。あるいは、まったく影響はないかもしれません。デジタル化が進む世界で生きている子供たちのデータという“お荷物”にはどんな物が入っているのでしょうか。おそらく、大抵は無害でつまらないものだと思いますが、中には人生を好転させる素晴らしいものもあるでしょう。反対に、足かせとなるものも入っているかもしれません。残念ながら、未来の大人の多くは、意図していなかったとしても、デジタルのお荷物に悩まされることになると予想します。

保護者は、子供たちがこの新しい世界を上手く生きていけるようにサポートしなければなりません。この世界では、子供たちはお腹の中に宿った瞬間から追跡され得るのです。2012 年、ある少女が自分でも妊娠に気づかないうちに、あるお店から妊娠関連商品のクーポンを受け取ったという話を思い出してください。

子供たちを守るためには、どのようなデジタル データが取得され、保存されているのかを理解する必要があります。全般的に、同意して利用するコンテンツ、未承諾利用コンテンツ、漏洩リスクのあるコンテンツの 3 種類があります。

同意して利用するコンテンツとは、利用規約やユーザー使用許諾契約の「同意します」ボタンをクリックした後に発生するすべての事柄です。最近発生したデータ漏えいを踏まえると、オンライン上に保存されるものは、いずれ必ずハッキングされます。ならば、最初からハッキングされることを想定するべきです。未来の雇用主が本当に望めば、採用候補者が過去に作成したコンテンツや、SNS でのふ

るまい、その他のデータ を探し出すことは可能かもしれません。これは、保護者が（少なくとも、最初は）適切なふるまいを教え、自らが見本となることで、十分にコントロールできるものです。10 歳の子供に 17 歳以上が対象のゲームを買い与えていないですか？あるいは、10 代の子供に親の監視なしで動画を投稿させてはいないですか？悲しいことに、インターネット上で起きたことはもうプライベートではなく、いずれ何らかの影響を受けることになるかもしれないのです。

未承諾利用のコンテンツとは、行動や発言が写真や動画に撮られたり、何らかの方法で文書化されたりして、インターネット上に公開されたコンテンツを意味します。飲酒やドラッグなどの愚かな行為だけでなく、公共の場やインターネット上で発言、投稿、ツイートした内容も含まれます。将来的に、（子供の）子供っぽい行動が攻撃材料として利用されることはないと思うので、そうした行動を制限する必要はないでしょう。

危険なのは、漏えいリスクのあるコンテンツです。私的なものと意図していたコンテンツや、取得されることを予想していなかったコンテンツのことです。残念ながら、より多くのユーザー情報を取得するため、さまざまな組織で、（誤って、または意図的に）自社のプライバシー ポリシーを捻じ曲げたり、違反を犯したりして、不慮の漏えいコンテンツを獲得することが常態化しています。玩具、タブレット、テレビ、インターフォン、その他のデバイスにかかわらず、誰かが子供の言葉や行動に関する情報を取得し、それをクラウドに送信しています。これは、デジタル生活における最大の課題であり、慎重に管理しなければならない部分です。購入やインストールするものに注意を払い、不要な機能は無効にし、初期設定パスワードは見破られにくいものに変えてください。

子供たちには、素晴らしいガジェットやアシスタント デバイス、体験に溢れた素晴らしい未来が待っています。その輝かしい未来に向けて、家庭内でデジタル コンテンツのメリットを最大化できるようにするため、データというお荷物の中身を適切に整理整頓する方法を教育しましょう。

企業側に関しては、今後のユーザー データや SNS の投稿などユーザーが作成したコンテンツの扱いに関する基準を定めるにあたり、2018 年 5 月に施行される EU 一般データ保護規制（GDPR）が重要な役割を果たすのではないかと予想しています。この新規制は、ヨーロッパ諸国でビジネスを展開している企業や、ヨーロッパに居住する人の個人データを扱う企業に影響します。つまり、世界中の企業がユーザーの個人データを処理、保存、保護する方法を調整しなければならなくなります。未来を見据えた企業は、この規制を活かし、家電、コンテンツ作成成可能なアプリのプラットフォーム、またその裏側のオンラインのクラウド ベース サービスの利用者に恩恵のあるベスト プラクティスを設定することができるでしょう。この点について、2018 年は、ユーザーに忘れ去られる権利があるかどうかについて考えさせられる象徴的な一年となるかもしれません。

企業のデータ保護の機会については、マカフィーの GDPR 関連サイト https://www.mcafee.com/jp/solutions/gdpr.aspx をご覧ください。

ユーザー作成コンテンツの乱用やその他のデジタル脅威から子供を守る方法については、デジタル時代の保護者のためのガイダンスに関して記載されたマカフィーのブログをご覧ください。

McAfee について

McAfee は、世界で最先端のサイバーセキュリティ企業です。McAfee では、より安全なデジタル世界を構築するため、個々の力を結集し、企業と個人を保護するソリューションを提供しています。他社の製品と連携するソリューションを構築することで、真に統合されたサイバーセキュリティ環境を整備し、脅威の対策、検出、修復を連動して行うことができます。McAfee の個人向けのソリューションは、すべての種類のデバイスに対応しています。自宅でも外出先でも、安心してデジタル ライフを楽しむことができます。McAfee では、他のセキュリティ企業との連携を強化し、力を合わせてサイバー犯罪者と戦っています。

www.mcafee.com/jp

McAfee Labs について

McAfee Labs は世界で最先端の脅威研究機関で、脅威情報やサイバーセキュリティに関する最新の情報を提供しています。世界各地に配備した数百万台のセンサーからデータを収集し、ファイル、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、リアルタイムで脅威情報、重要な分析結果、専門的な情報を提供し、保護対策の向上とリスクの軽減に貢献しています。

https://www.mcafee.com/jp/mcafee-labs.aspx

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティウエスト 20F
www.mcafee.com/jp