キーサイト・テクノロジー株式会社
〒192-8550 東京都八王子市高倉町9-1
www.keysight.co.jp

報道関係者からのお問い合わせ
キーサイト・テクノロジー株式会社
広報担当 土肥（どひ）
電話：042-660-2162

お客様からのお問い合わせ
キーサイト・テクノロジー株式会社
計測お客様窓口
電話：0120-421-345

※このお知らせは、米国時間2021年4月21日にキーサイト・テクノロジーズ・インクが発表したニュースリリースを、キーサイト・テクノロジー株式会社が和訳・要約したものです。

キーサイト、ネットワークセキュリティに関する重大な 3 つの懸念事項を「2021 年セキュリティレポート」で発表

脅威には、パンデミックによるフィッシングの傾向、ランサムウェア、重大なセキュリティサプライチェーンの脆弱性が含まれると報告

東京、2021 年 5 月 17 日発 – イノベーションを加速し、あらゆるものが安全につながる世界を実現する高度な設計と検証ソリューションを提供する、キーサイト・テクノロジーズ・インク（CEO：ロン・ネルセシアン、米国カリフォルニア州サンタローザ、NYSE：KEYS、日本法人：キーサイト・テクノロジー株式会社、以下「キーサイト」）は、第 4 弾となる「Keysight セキュリティレポート」を発表しました。2021 年版レポートでは、キーサイトの Application and Threat Intelligence（ATI）リサーチセンター による過去のセキュリティトレンドに加えて、ネットワークセキュリティに関する 3 つの懸念事項を記載しています。

今回のレポートでは、ネットワークセキュリティテストにおけるキーサイトの幅広い経験と、ネットワークおよびクラウドの可視化に対する専門知識が活かされています。キーサイトの ATIリサーチセンターは、世界各地のサイバーセキュリティ専門家チームで構成されており、エンタープライズITネットワークのセキュリティを脅かす恐れがある、進化し続ける痕跡のモニターと解析を行っています。世界中に置かれたハニーポット、チームによる独自調査、国際的なエクスプロイトデータベース、ダークウェブ、セキュリティニュースのアラートのスキャン、クラウドソーシング、ソーシャルメディア、パートナーフィードなど、複数の情報ソースを調査プロセスに活用しています。

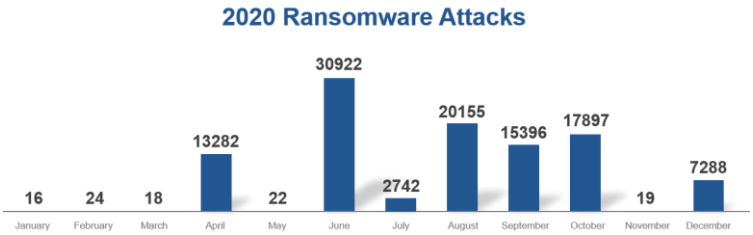
キーサイトのセキュリティソリューション担当シニアバイスプレジデントのScott Registerは、次のように述べています。「このレポートは、2020年に得られた教訓と、2021年のネットワークセキュリティ専門家に向けた洞察を組み合わせたものです。データも洞察も、キーサイトのATIリサーチセンターが実施した調査を元にしています。サイバー犯罪は、パンデミック（世界的大流行）の最中も休むことなく行われました。サイバー犯罪者は、フィッシング、ランサムウェア、サプライチェーンベクトル攻撃を利用して、ネットワークに打撃を与え、金銭的な利益を手にしています。このようなネットワークセキュリティの傾向は、2021年も続くと考えられます。」

2020年のサイバー犯罪のトレンドには3つの特徴がありました。

- **フィッシング攻撃は62%増加した。**キーサイトの調査によると、2020年のフィッシング攻撃は、2019年と比べて62%増加しています。実際、3月と4月にパンデミックが起きると、これらの攻撃

は急増しています。これはソーシャルエンジニアリング攻撃がパンデミックと関係していたためです。

- **金銭的な利益が、サイバー犯罪の主な動機として注目を集めた。**ランサムウェアは、6月に大きく増加しました。この傾向はすべての業界に共通したものですが、医療関係が特に大きな打撃を受けました。こうした攻撃の59%は、2020年下半期に発生しています。



- **サプライチェーン攻撃は、SolarWinds の攻撃で大きく報じられた。**
サプライチェーンは依然として弱点となっており、SolarWindsへの攻撃により、セキュリティアーキテクトが全体的で包括的なアプローチを取る必要性がさらに強まっています。

Keysight 2021 セキュリティレポート の戦略的洞察（Strategic Insights）

戦略的洞察 #1:
フィッシングやその他ソーシャルエンジニアリング攻撃は、パンデミック関連のニュースを利用して今後も行われるでしょう。
キーサイトの提言：人々はソーシャルエンジニアリングによるワクチン詐欺を認識する必要があります。また、ネットワークセキュリティチームは、悪質な業者が医療および政府機関の個人識別情報（PII）を標的としていることを認識する必要があります。

戦略的洞察 #2:
ランサムウェアは、大きな資金源となるため悪質業者が頻繁に悪用します。この不正行為がなくなることはなく、ビジネスモデルは今後もマルウェアの変種とともに現れてくるでしょう。
キーサイトの提言：ランサムウェア作成者は、難読化や検知回避に長けているため、企業の脅威検知システムを最新のシグニチャと行動パターンで常に最新の状態に保つことが重要です。さらに、ネットワークセキュリティチームは、エクスプロイトプラクティスが進化していることも認識する必要もあります。

戦略的洞察 #3:
組織のサプライチェーンは単なる構成要素ではありません。サプライチェーンとは、製品製造時に使用するソフトウェアやハードウェアコンポーネントを供給する外部組織として考える傾向があります。
キーサイトの提言：サプライチェーンは、ユーティリティ、Eメール、クラウドプロバイダーから、コーヒーサプライヤーも含め、ビジネスの運用には不可欠です。ネットワークセキュリティは、組織と IT システムに影響を与える可能性がある、従来とは異なる構成要素も考慮する必要があります。

戦略的洞察 #4:
ゼロトラストは、単なる流行語ではありません。ユーザーが組織のネットワークに接続したときに表示される内容を制限するわけではありません。
キーサイトの提言：ゼロトラストの実装を成功させるには、システムとユーザーが確実に必要とする内部または外部リソースのみにアクセスできる必要があります。

戦略的洞察 #5:
組織が侵害され、それに応じた行動することを想定します。
キーサイトの提言：組織には、自身のネットワークとクラウドリソースへの可視化が必要です。ネットワークセキュリティチームがネットワーク（オンプレミス、クラウド、リモートユーザーを問わず）に隠された異常を特定できない場合、侵害がいつまでも検知されないままになります。

キーサイト・テクノロジー株式会社
〒192-8550 東京都八王子市高倉町9-1
www.keysight.co.jp

Keysight 2021 セキュリティレポートの概要は キーサイトのニュースルームをご覧ください: www.keysight.com/find/security-report-2020

レポート全文はこちらをご覧ください: www.keysight.com/jp/ja/assets/3121-1093/white-papers/Keysight-Technologies-2021-Security-Report.pdf

キーサイト・テクノロジーについて

キーサイトは、イノベーションを加速し、あらゆるものが安全につながる世界の実現を支援する高度な設計と検証ソリューションを提供しています。キーサイトのスピードと精度へのこだわりは、ソフトウェアドリブンな洞察と分析にまで及び、設計シミュレーションから、プロトタイプ検証、自動化ソフトウェアテスト、製造解析、さらにエンタープライズ、サービスプロバイダーおよびクラウド環境でのネットワークパフォーマンスの最適化と可視化など、開発ライフサイクル全体にわたり、明日に向けたテクノロジー製品をより迅速に市場に投入することを可能にしています。当社のお客様は、世界各国の通信と産業エコシステム、航空宇宙／防衛、自動車、エネルギー、半導体、一般電子機器など、多岐にわたっています。2020 年度の売上高は、42 億ドルでした。キーサイト・テクノロジー(NYSE: KEYS)に関する詳細情報は、こちらをご覧ください。www.keysight.co.jp

# # #

キーサイト・テクノロジーに関するその他の情報は、www.keysight.com/go/news のニュースルーム、Facebook、LinkedIn、Twitter、YouTube でご覧いただけます。

PRJ20_NR21036