報道関係者各位

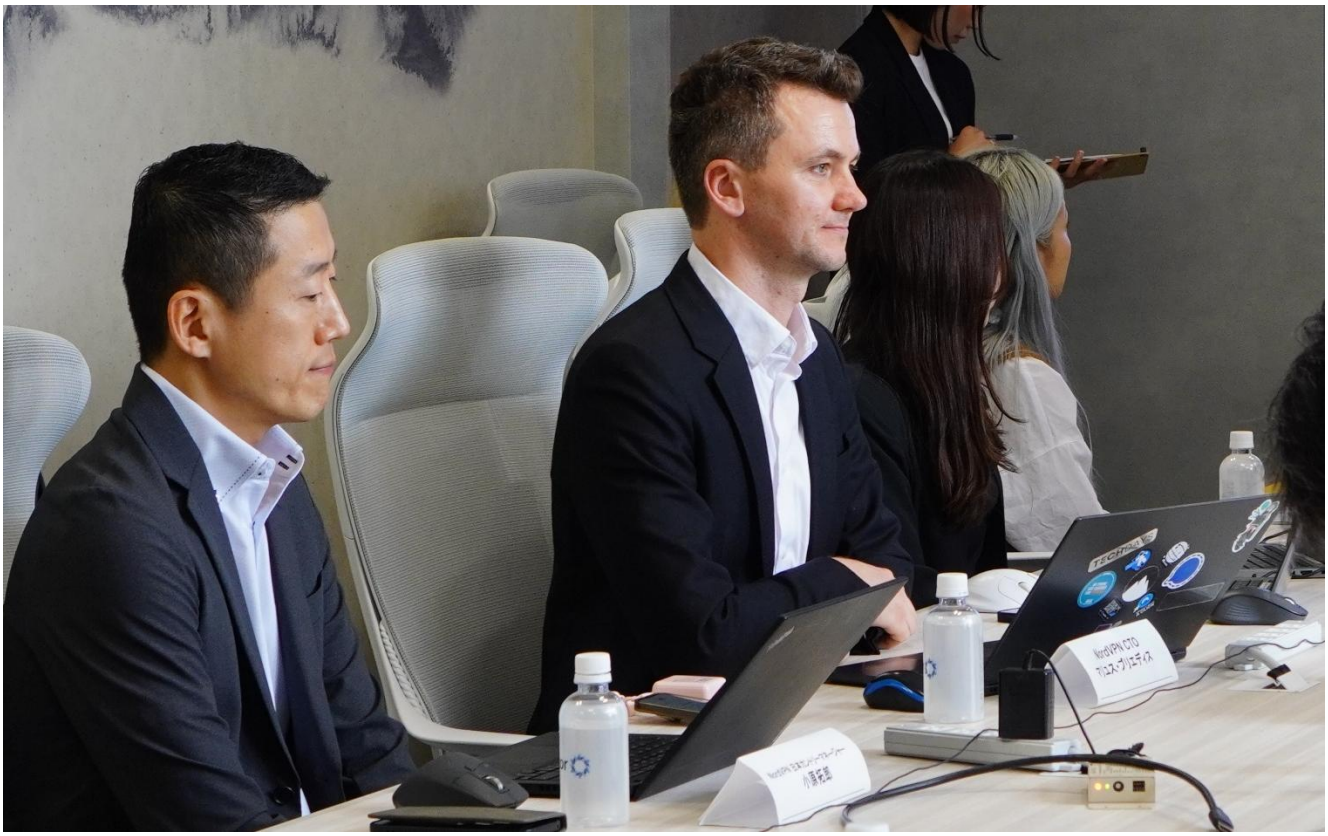
2025 年 10 月 16 日

NordVPN がメディアラウンドテーブルを開催、来日した CTO が日本の「無自覚な」サイバーリスクに警鐘

～最新調査で、日本のビジネスパーソンの約半数が危険な行動をとっている実態が明らかに～

個人向けセキュリティサービスを提供する NordVPN（本社：オランダ・アムステルダム、日本代表：小原拓郎）は 2025 年 10 月 7 日（火）に、最高技術責任者（CTO）のマリユス・ブリエディスと日本代表の小原拓郎が登壇するメディア向けラウンドテーブルを都内で開催し、日本市場向けの最新調査結果を発表しました。

本イベントでは、日本のビジネスパーソン 1,000 名を対象とした最新のサイバーセキュリティ意識調査の結果が発表され、多くの人が自身のセキュリティを過信し、無意識のうちに深刻なリスクに晒されている実態が明らかになりました。この結果を受け、マリユスと小原が日本のメディアと議論を交わし、なぜ日本では“知識と行動のギャップ”が生まれるのか、その背景と対策について、グローバルな視点から活発な議論が展開されました。



画像左：NordVPN 日本代表 小原拓郎　画像右：NordVPN　最高技術責任者（CTO） マリユス・ブリエディス

■NordVPN のビジョンと進化を続ける最新技術

イベントは、「誰もが自由で安全なインターネットを利用できる環境を実現したい」という Nord Security の紹介から始まりました。その中核をなす「NordVPN」は、単なる VPN 製品から「サイバーセキュリティの総合的なアプリケーション」へと進化し、通信の暗号化や厳格なノーログポリシーといった基本機能に加え、常に最先端の技術を導入しています。

CTO のマリユスは、その代表例として 3 つの最新技術を紹介しました。独自の AI（特許取得済み）を活用し、マルウェアやフィッシングサイトを未然にブロックする「脅威対策 Pro™」機能のほかに、将来の量子コンピュータによる解読リスクに備える「耐量子暗号化（PQC）」の全アプリへの導入、さらに VPN 通信を通常の Web ブラウジングのように見せかけ、ネットワークによる検知・ブロックを回避する独自プロトコル「NordWhisper」も紹介しました。これらの先進技術と、大手監査法人 Deloitte Audit Lithuania（デロイト・オーディット・リトアニア）による 5 回目のノーログ監査認証で、NordVPN の信頼性を支えています。

■最高技術責任者マリユスが警鐘を鳴らす、日本のビジネスパーソンに潜む「落とし穴」

本イベントの核心として、日本のビジネスパーソン 1,000 名を対象とした最新調査の結果が発表されました。CTO のマリユスは、グローバルな視点から日本の特異性を指摘し、警鐘を鳴らしました。

- **意識と行動の深刻なギャップ**：回答者の約半数（47%）が無意識に危険な行動をとっており、特に自身のセキュリティに「自信がある」と回答した人ほどリスクの高い行動を取る傾向が明らかになりました。
- **長時間労働者のリスク**：月 40 時間以上残業する人は、公共 Wi-Fi の利用率が平均の 2.3 倍に達するなど、多忙な中でセキュリティ対策が疎かになる実態が浮き彫りになりました。
- **見過ごされる自宅の Wi-Fi ルーター**：6 割以上が自宅の Wi-Fi ルーターの対策が不十分であり、23%が ID やパスワードを初期設定のまま使用。CTO のマリユスは「ルーターへのハッキングは非常に危険であり、OS やアプリと同様にアップデートが不可欠です」と強く訴えました。
- **ダークウェブに流出する膨大なクッキー情報**：今年ダークウェブ上で観測された 940 億点以上のクッキーのうち、2 億 5,000 万点以上が日本から流出したものでした。さらに、そのうち 2,000 万点は現在もアクティブな状態にあり、攻撃に悪用される危険性があると報告されました。

■日本特有のセキュリティ課題

質疑応答のコーナーでは、活発な議論が交わされました。日本のビジネスパーソンが見過ごしがちな具体的なセキュリティの課題について、マリユスが専門的な見地から見解を述べました。

HTTPS 通信の普及により、現代における公共 Wi-Fi のリスクについても安全と思われがちですが、マリユスは「通信の一部が暗号化されるだけで、他のアプリ通信は保護されません。古いプロトコル（TLS 1.2）ではトラッキングも防げず、十分ではありません」と回答しました。通信の『経路』だけでなく『両端』のデータ保護も重要」と、カフェや空港などでデータを盗み見る中間者攻撃のリスクを避けるため、VPN による通信全体の暗号化が依然として不可欠ですと強調しました。

また、企業におけるデータ損失防止（DLP）が最大の課題の一つであると指摘し、「社員が業務データを個人クラウドや生成 AI に持ち出すリスクに対し、技術的な対策と並行して、継続的な社員への啓蒙と教育が最も重要だ」と述べました。マリユスは、社員一人のデバイスのウィルス感染が企業全体に与える影響について、「セキュリティの強さは“最も脆弱なリンク”で決まる。個人のデバイスが感染すれば、会社のネットワーク全体が危険に晒される」と語り、組織における個人のセキュリティ意識の重要性を強調しました。

さらに、日本で数千億円規模の被害が報告されている投資詐欺やロマンス詐欺についても、「脅威対策 Pro™」機能が既知の悪質なリンクやウォレットアドレスをブロックすることで、こうした詐欺被害を未然に防ぐ一助となると言及しました。

■NordVPN 最高技術責任者 マリユス・ブリエディス のコメント

「セキュリティリスクを認識していても、それが必ずしも安全な行動につながるわけではありません。公共 Wi-Fi やブラウザの自動保存が危険だと理解していても、利便性が優先されてしまうことは多々あります。こうした“近道”は一見無害に思えても、情報の窃取やデータ漏洩といったリスクを招く可能性があります。サイバーセキュリティは、日々の小さな行動にかかっています。自動保存の代わりにパスワードマネージャーを使用し、多要素認証を必ず有効にし、信頼できる VPN を利用するなど、こうした小さな心がけの積み重ねこそが、組織全体の安全を守る大きな力になります。今日のラウンドテーブルにて、VPN やパスワードマネージャー、そしてサイバーセキュリティ全般について、何か新しい発見があったなら嬉しく思います。皆様が今日からさらに安全にオンラインで活動されることと、日本のメディアの皆さんの力を借りて、この重要性をより日本の社会に伝えていけることを願っています。」

■NordVPN について

NordVPN は、世界中で何百万人ものユーザーをもつ先進的な VPN サービスプロバイダーです。8,200 台以上のサーバーを世界 127 カ国 165 都市で提供し、専用 IP や Double VPN、Onion Over VPN サーバーなど、多彩な機能を備え、トラッキングなしでオンラインプライバシーを強化します。主要機能の一つである「脅威対策 Pro」は、悪質なウェブサイトやトラッカー、広告のブロックに加え、マルウェアのスキャンが可能です。さらに、最新の製品であるグローバル eSIM サービス「Saily」を展開しています。「Saily」は海外旅行者向けに設計されており、現地で SIM カードを購入する必要がなく、簡単にデータ通信が利用可能です。

【会社概要】

会社名：NordVPN

本社：Fred. Roeskestraat 115 1076 EE Amsterdam, Netherlands

日本代表：小原拓郎

NordVPN ウェブサイト：https://nordvpn.com/ja/

VPN について：https://nordvpn.com/ja/what-is-a-vpn/