

CrowdStrike CEO、 コロナウイルスがもたらす サイバーセキュリティへの 影響に対する取り組みを語る

20 March 2020 | George Kurtz (CrowdStrike)

まず、医療従事者、法執行機関、初動要員のみなさま、ならびに市民の安全と健康のために自身を危険にさらして働いてくださっているすべての方に、世界各地の CrowdStrike® チームを代表して、感謝の念を送りたいと思います。また、ご家族や愛する方々がこの壊滅的なウイルス大流行の影響を受けたすべての人にお見舞い申し上げます。

CrowdStrike の CEO としての私の第一の責任は、共に生活や仕事をしている人々およびコミュニティにあります。そのため、私は CrowdStrike の全従業員に対し、在宅勤務に切り替え、不必要な出張をやめることを指示し、この非常に感染性の高い病気の蔓延を遅らせるべく、すべての地方および国家の健康指針を順守するように働きかけました。現時点では、COVID-19 感染の診断を受けた当社従業員はいないということをご報告するとともに、今後もこの状態を維持したいと考えています。

私たちの次の責任はもちろんお客様に対するものであり、それに関する多くの進展についてもお伝えしたいと思います。ここで明確にしておきたいことがひとつあります。それは、CrowdStrike がこの危機において、非常に重要な役割を担っているということです。

コロナウイルスは健康と経済に広範囲な悪影響を与えていますが、サイバー攻撃は抑止されてはいません。実際、まったく逆のことが起きています。世間が危機に瀕している時、攻撃者らがその状況を悪用することがよくあります。人々の恐怖に付け込んで、攻撃をエスカレートさせるのです。信じられないことですが、当社はすでに、国家主導の攻撃者グループやサイバー犯罪者らがコロナウイルスに便乗して仕掛けたフィッシング攻撃を発見しています。私たちはこのような攻撃の増大を予想しており、コロナウイルスそのもののように拡大する悪質な活動を追跡しています。

当社の革新的なクラウドネイティブのアプローチは、従業員が自宅にいても、オフィスにても、あるいは完全にクラウド内で業務を行っていても、企業がこのような新出の脅威より一歩先んじることができるよう支援します。

私たちのコミュニティ支援を当社のお客様にまで拡張すべく、このたび **コロナウイルス・サージ・リリーフ・プラン** を開始しました。これは、当社のお客様に CrowdStrike Falcon® プラットフォームで保護していただけるエンドポイントの数を、最大 60 日間拡張するものです。これにより、既存のお客様は、調達サイクルを心配することなく、新しいリモートワーカーをすばやくオンボードさせることができます。合わせて **CrowdStrike Falcon Prevent™ for Home Use プログラム** も開始しました。こちらを利用いただく事で、管理者の方は期間限定で当社の次世代型エンドポイント保護を、従業員の個人用システムにもすぐにインストールできるようになります。このような緊急時において、これらの無料プログラムは、お客様に非常に高く評価されています。

どのような規模、業界、所在の組織であれ、従業員の在宅勤務をすぐに開始可能にするのは容易なことではありません。特に大規模な組織では、そのような新体制を迅速かつ効率的に管理することは非常に困難であると思われる。CrowdStrike は、この点において安心です。なぜなら、私たちは当初からリモートで働く従業員とともに成長してきた会社だからです。当社では、日頃から約 70% の従業員が在宅勤務を行ってきました。そのため、残りの従業員をテレワークモデルに切り替えても、当社の業務やお客様へのサポートに混乱をきたすことはないはずで

多くのお客様にとって、リモートへの移行はそれほど単純なことではありません。従業員を物理的なオフィスの外に移動させると、攻撃対象領域が指数関数的に増大することに十分注意しなければなりません。移行にあたっては、ノート PC やモバイルデバイスなどの新しいエンドポイントを速やかにプロビジョニングして、新たなクラウドワークロー

ドを構成し、どのワークロードも、たとえユーザーがオフラインであっても、リアルタイムに保護できるようにする必要があります。

具体的な例では、当社の大企業のお客様は、最近ノート PC 12,000 台を急速購入し、リモートの従業員用に展開しました。CrowdStrike は、この種の導入展開において重要な役割を果たすことができます。なぜならば、リモートワークに伴うセキュリティ上の問題は、クラウドネイティブのセキュリティプラットフォームで解決するのがベストであるからです。CrowdStrike Falcon のような真のクラウドネイティブのプラットフォームでは、物理的なインフラストラクチャーは不要です。お客様は、従業員の働く場所に関係なく、大規模なワークロード環境におけるインストール、管理、保護をリモートから容易に行うことができます。

このような状況下でも、トップ企業は顧客の成功に寄与すべく革新を続けています。それにより、企業もその顧客も危機を脱し、さらなる増強が実現されるでしょう。企業がビジネスのレジリエンシーを実現し、その従業員や顧客が安心して個々の重要な業務に集中し続けることができるためには、これまででも、そしてこれからも、サイバーセキュリティが必要不可欠です。

この難しい状況下において、皆さまの組織の安全確保のために CrowdStrike ができることがあれば、遠慮なくご連絡ください。CrowdStrike には標語があります。「ワンチーム。ワンファイト。」 私たちは一丸となって闘います。



George Kurtz (CrowdStrike)

追加のリソース

- COVID-19 蔓延時におけるサイバーセキュリティ上の課題や、リモートワーカーの安全のための推奨事項に関する詳細については、[CrowdStrike の CTO、Mike Sentonas](#) および [チーフプロダクト・エンジニアリング・オフィサーの Amol Kulkarni](#) のブログをご覧ください。
- [CrowdStrike COVID-19 リソース Web ページ](#) をご覧になり、御社とリモートワーカーのセキュリティ確保に役立つ情報を入手してください。
- オンデマンド Web キャストもご覧ください。[『Cybersecurity in the Time of COVID-19 \(新型コロナウイルス蔓延時代のサイバーセキュリティ\)』](#)