中小企業・組織にも平等にゼロトラストへのアクセスを

上記の地域で資格を満たす企業・組織は、エンタープライズレベルのゼロトラストサイバーセキュリティサービスを利用できるほか、DDoS 攻撃対策、Web アプリケーションファイアウォール（WAF）など、世界トップレベルのアプリケーションセキュリティ製品を無料で利用可能になります。これによって、リスクにさらされている重要インフラ企業・組織が以下の内容を実現できるようになります。

- **ユーザーとアプリケーションのリアルタイム接続：**すべてのアプリケーションにおいて、全ユーザーをリアルタイムに検証することで、内部リソースを保護するとともに、潜在的なデータ漏洩を防止します。
- **トラフィックのフィルタリング：**セキュア Web ゲートウェイ（SWG）は、Web トラフィックから不要なコンテンツをフィルタリングし、不正なユーザー行為をブロックします。さらに、企業・組織のセキュリティポリシーを適用することで、サイバー脅威やデータ漏洩を防止します。
- **セキュアなクラウドアプリケーション：**クラウドアクセスセキュリティブローカー（CASB）は、SaaS、IaaS、PaaS などクラウドでホストされるサービスに対して、複数のセキュリティ機能を実行します。標準的な CASB の機能には、アクセス制御とデータ損失防止対策（DLP）による機密性の高いデータ保護、シャドーIT（非承認システム）の特定、データプライバシー規制の確実な順守などが備わっています。
- **機密データ保護：**Data Loss Prevention（DLP）は、企業・組織のもっとも重要な機密データを転送する際に保護します。
- **フィッシング攻撃防止：**Area 1 は、フィッシング、ビジネスメール詐欺、マルウェアレス詐欺など、メールを介して絶え間なく行われる攻撃や脅威を先制的にブロックします。

「Project Safekeeping」の参加資格としては、非営利団体、地方自治体、および、地域社会の健康、安全、基本的な経済ニーズに不可欠なサービスの提供を主な事業内容としている中小企業・組織である必要があります。

詳細については、以下のリソースをご覧ください。

Project Safekeeping – protecting the world's most vulnerable infrastructure with Zero Trust
http://blog.cloudflare.com/project-safekeeping

Project Safekeeping: Zero Trust cybersecurity for critical infrastructure
https://www.cloudflare.com/lp/project-safekeeping/

Cloudflare Impact Week 2022
https://www.cloudflare.com/ja-jp/impact-week/

Zero Trust へのロードマップ
https://www.cloudflare.com/ja-jp/learning/insights-roadmap-zerotrust/

Cloudflare（クラウドフレア）について

Cloudflare, Inc.（ https://www.cloudflare.com/ja-jp/ /@cloudflare）の使命は、より良いインターネットの構築をサポートすることです。Cloudflare のプラットフォームは、ハードウェアやソフトウェアの追加、コードの変更を行うことなく、あらゆるインターネットアプリケーションを保護、高速化します。Cloudflare により、インターネットプロパティのすべてのトラフィックがインテリジェントなグローバルネットワークを経由してルーティングされ、リクエストを受け取るたびにスマートになります。その結果、パフォーマンスが大幅に向上し、スパムその他の攻撃が減少します。Cloudflare は「アントレプレナー」誌の Top Company Cultures 2018、「Fast Company」誌の 2019 年版 World's Most Innovative Companies に選出されました。

将来予想に関する記述

本プレスリリースには、将来予想に関する記述（1933 年米国証券法第 27A 条および 1934 年米国証券取引所法 21E 条（いずれもその後の改正を含む）に該当）があり、それらには重大なリスクおよび不確定要因が含まれています。将来予想に関する記述は、「場合があります」、「つもりです、するでしょう」、「はずです」、「見込まれます」、「可能性を探ります」、「する計画です」、「予想します」、「かもしれません」、「意図しています」、「目標とします」、「見積ります」、「検討します」、「考えます」、「推測します」、「予測します」、「潜在的」、「引き続き」、ないしはそれらの否定表現、あるいは当社の予想、戦略、計画、または意図に関わるその他同様の用語もしくは表現によって識別することができます。しかし、すべての将来予想に関する記述にこうした語句が含まれているわけではありません。本プレスリリースで明示または黙示されている将来予想に関する記述には、次を含みますが、これらに限定されません。重要インフラストラクチャ組織が Cloudflare の Zero Trust、アプリケーションセキュリティ、その他の製品およびテクノロジーを使用することで得られる潜在的メリット。Cloudflare の Zero Trust、アプリケーションセキュリティ、その他の製品およびテクノロジーの性能と有効性。Cloudflare の Zero Trust、アプリケーションセキュリティ、その他の製品およびテクノロジーの使用によって得られると期待される機能とパフォーマンス。Cloudflare の Zero Trust、アプリケーションセキュリティ、その他の製品およびテクノロジーの新機能が、Cloudflare のすべてのお客様（現行および見込み）に一般公開されるタイミング。Cloudflare の技術開発、将来の運用、成長、イニシアチブ、または戦略。Cloudflare の CEO その他のコメント。Cloudflare が 2022 年 11 月 3 日に米国証券取引委員会（SEC）に提出した四半期報告書（フォーム 10-Q）や当社が SEC に随時提出するその他の文書で詳説するリスク（ただしこれらに限定されない）をはじめ、さまざまな要因によって、上記の将来予想に関する記述で明示または黙示した結果と実際の結果との間に重大な相違が生じる可能性があります。Cloudflare が 2022 年 11 月 3 日に米国証券取引委員会（SEC）に提出した四半期報告書（フォーム 10-Q）や当社が SEC に随時提出するその他の文書で詳説するリスク（ただしこれらに限定されない）をはじめ、さまざまな要因によって、上記の将来予想に関する記述で明示または黙示した結果と実際の結果との間に重大な相違が生じる可能性があります。

本プレスリリースに含まれる将来予想に関する記述は、あくまで記述当日現在の事象についてのみ言及しています。当社は、法律によって義務付けられている場合を除き、本プレスリリースの日付以降の事象や状況を反映するために、あるいは新しい情報や予期しない事象の発生を反映するために、将来予想に関する記述を更新する義務を負いません。Cloudflare が将来予想に関する記述で開示した計画、意図、予想は実際に実行・達成されない場合があるため、Cloudflare の将来予想に関する記述に過剰に依存すべきではありません。