連邦政府によるサイバー攻撃及び対策に関する注意喚起

２０２０年6月１９日
ブリスベン総領事館

モリソン首相は，６月１９日の会見で，官民問わず様々な機関に対する特定の国家を基礎とする主体による巧妙なサイバー攻撃が増大していることを明らかにし，その対策について専門的助言を得るとともに，サイバー攻撃から自らを守るための防護的措置を講じるよう注意喚起を行いました。

１　モリソン首相等による注意喚起の概要

（１）モリソン首相は，６月１９日の緊急会見で，現在，豪国内の官民問わず多くの機関が特定の国家を基礎とする巧妙なサイバー主体から継続的な攻撃の対象とされており，連邦・州・地方政府，産業界，政治組織，教育，医療保健，消防・警察等必須サービス提供者及び重要インフラ運営者を含む広範な分野に対しサイバー攻撃が行われている旨述べました。

（２）同首相は，このような攻撃が増大しつつあるとして，このようなリスクと特定の標的を狙う攻撃活動を認識し，サイバー対策について専門的助言を得るとともに，サイバー攻撃から自らを守るための防護的措置を講ずるよう注意喚起を行いました。

（３）モリソン首相とともに会見したレイノルズ国防大臣は，豪州サイバー・セキュリティ・センター（ACSC）等が，豪国内の関係機関がサイバー脅威を探知し軽減することを可能とするためのサイバー対策に関する技術的助言を取り纏め公表した旨述べました。これら助言の概要については以下２を参照ください。

モリソン首相のメディア声明（原文）については，以下のリンクをご覧ください。
https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

２　参照すべきサイバー対策の概要

（１）ACSC から被害軽減のために優先的に行うべき対策として指摘されているのは，以下の２点です。また，最新のサイバー脅威注意情報を入手し，なるべく早くオンライン上で自らを守るための措置を執ることが可能となるよう，ACSC のパートナーとなることを推奨しています。

●インターネットに接続しているインフラについて，可及的速やか（４８時間以内）にセキュリティ・パッチや被害軽減対策を適用し，可能な限り最新のソフトウェア及び OS を使用する。

●インターネットで遠隔操作できるサービス（ウェブメール，クラウドメール，コラボレーション・プラットフォーム，VPN，リモート・デスクトップ・サービス等）には，多要素認

証（パスワードのみならず，デバイスや生体情報など複数の要素で認証）を活用する。
詳細については，以下のリンクをご参照ください。
https://www.cyber.gov.au/news/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks
（２） 他の被害軽減対策として，ACSC は「Essential Eight」と題した対策を推奨しています。
詳細については，以下のリンクをご覧ください。
https://www.cyber.gov.au/publications/essential-eight-explained

３　サイバー攻撃を受けた場合の報告等
（１）連邦政府は，万一サイバー攻撃の被害者となった場合，以下のＵＲＬにアクセスし，報告を行うよう呼びかけています。
https://www.cyber.gov.au/report
（２）また，サイバー・セキュリティ案件について助言を必要とする場合，以下のメールアドレスに連絡するよう呼びかけています。
asd.assist@defence.gov.au

このメールは，在留届にて届けられたメールアドレスおよび「たびレジ」に登録されたメールアドレスに自動的に配信されております。
＜問い合わせ先＞
在ブリスベン日本国総領事館
住所：Level 17, 12 Creek Street, Brisbane QLD 4000
電話：07 3221 5188 / FAX 07 3229 0878
※「たびレジ」簡易登録をされた方でメールの配信を停止したい方は，以下のURL から停止手続きをお願いいたします。
https://www.ezairyu.mofa.go.jp/tabireg/simple/delete