National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

オンラインで組織の安全を守る

なぜサイバーセキュリティはコミュニティグループや組織にとって重要なのでしょうか?

本書では、コミュニティグループや組織をサイバーセキュリティの脅威から保護するためのアドバイスといくつかの対策について説明します。なお、個人がオンラインで安全を確保するための案内も別途準備しています。

このアドバイスは、最も一般的で深刻な脅威を考慮して作られたものです。

- アップデートでデバイス上のソフトウェアを最新の状態にし、セキュリティの抜け穴にパッチを当てます。
    - コミュニティグループや組織のデバイスを最新の状態にしましょう。デバイスとは、電話、コンピューター、WiFi ルーターなど、インターネットに接続する全ての機器を指すもので、スマートデバイスも含みます。
    - 可能な限り、自動更新でアップデートをしてください。
- 二要素認証(2FA)とはパスワードと、携帯電話のアプリでのコードなど、もう 1 つのステップを要求することで、アカウントのセキュリティ強化に有効な手段です。
    - 多要素認証(MFA)、2 段階認証(2SV)など、他に多くの名前で呼ばれることもあります。
    - すべてのコミュニティグループや組織のアカウントで 2FA をオンにしてください。
    - 騙されてログイン情報を開示しないように、可能ならフィッシングに強い 2FA の形式を使用すると良いです。指紋や顔認証など、物理的なセキュリティキーを使うこともできます。
- オンラインアカウントを管理してください。コミュニティグループや組織を退会した元メンバーがグループや組織のアカウントへのアクセスができないようにすることが重要です。
    - 同じアカウントに複数のユーザーがアクセスしている場合は、全員が異なるログイン情報を使用し、全員が 2FA がオンになっているようにしてください。
    - すべてのユーザーアカウントのリストを保持し、メンバーの退職時など、不要なアカウントはすべて削除してください。
    - メンバーに譲渡したデバイスの登録情報を保管し、その人が組織を離れる場合は、デバイスを返却してもらうことを忘れないようにして、返却されたデバイスを工場出荷時の状態にリセットします。また、建物のアクセスに関するコードを変更する必要になる場合もあります。
- オンラインアカウントにアクセスできるユーザーを確認してください。 コミュニティグループや組織のメンバーは、必要なものにのみアクセスできるようにすると有効です。
    - 1 人のアカウントがハッキングされた場合、この対応により被害を低減できます。

    - また、不要な権限を定期的に確認し、削除してください。
    - 複数のユーザーが使用する同一の「管理者」アカウントがある場合は、異常なアクティビティがないか監視する必要があります。特に日常のタスクにおいて、このようなアカウントを最小限にすると良いです。
    - これらのルールは、ルーターなどのデバイスへの管理者アクセスについても同じです。
- サービスプロバイダーに IT サービスの運営を依頼しているなら、その契約を確認してください。
    - コミュニティグループや組織のニーズを満たすサイバーセキュリティ保護が実施されていることを確認する必要があります。
- すべてのアカウントとシステムがどのように連携しているかを確認してください。接続方法を理解することによって、攻撃者がどこから侵入できるかを知ることができます。
    - メール、クラウドストレージ、会計プラットフォームなど、システム間の接続を確認すると良いです。
    - また、オンラインの安全性を高めるために、仮想プライベートネットワーク（VPN）の使用を検討することも有効です。VPN を使うと、追跡しようとする人からオンライン活動を隠すことができます。これは、コミュニティグループや組織のメンバーがリモートで接続する場合には特に効果的です。
- メンバーが「サイバースマート」である必要があります。コミュニティグループや組織のメンバーは、システム自体よりも標的にされる可能性が高いです。
    - すべてのスタッフに基本的なサイバーセキュリティのトレーニングを行ってください。「オンライン時は自分主導に」ウェブサイト Own Your Online |NCSC には、オンラインでの安全を確保し、詐欺に気付くためのさまざまなアドバイスとヒントがあります。
    - 組織で使用しているアカウントの他に、各々の個人アカウントについてもこれらの対応が重要であることを分かっていただくと良いです。
    - さらに、個人がオンラインで安全を確保するための案内を用意しています。
- インシデントに備えて対処手順を設定してください。インシデントが発生したときに対応に慌てないようにするには、予め対処手順を設定することが重要です。
    - インシデント対処手順の中で、インシデント発生時に誰が何をするかを設定します。テンプレートはこちらから入手できます。 インシデント管理 |NCSC
    - 電話、コンピューター、またはその他にシステムに障害が発生した場合の対処方法に関する手順も記載しましょう。また、対処手順を常に最新の状態にアップデートする必要もあります。
    - 必要なメンバー全員の連絡先の詳細を保管し、連絡する主な方法（電子メールなど）に障害があることも想定して、バックアップ連絡先の詳細を入れておきましょう。

- 対処プロセスにアクセスできない場合に備えて、システムの外部に保管してください。