参考資料２

特集1

２月1日～3月18日は「サイバーセキュリティ月間」です

サイバーセキュリティ対策９か条

1. OSやソフトウェアは常に最新の状態にしておこう
2. パスワードは長く複雑にして、他と使い回さないようにしよう
3. 多要素認証を利用しよう
4. 偽メールや偽サイトに騙されないように用心しよう
5. メールの添付ファイルや本文中のリンクに注意しよう
6. スマホやPCの画面ロックを利用しよう
7. 大切な情報は失う前にバックアップ（複製）しよう
8. 外出先では紛失・盗難・覗き見に注意しよう
9. 困った時はひとりで悩まず、まず相談しよう

出典：サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会「サイバーセキュリティ意識・行動強化プログラム」、2022年10月

「サイバーセキュリティ月間」なぜ2月1日～3月18日？

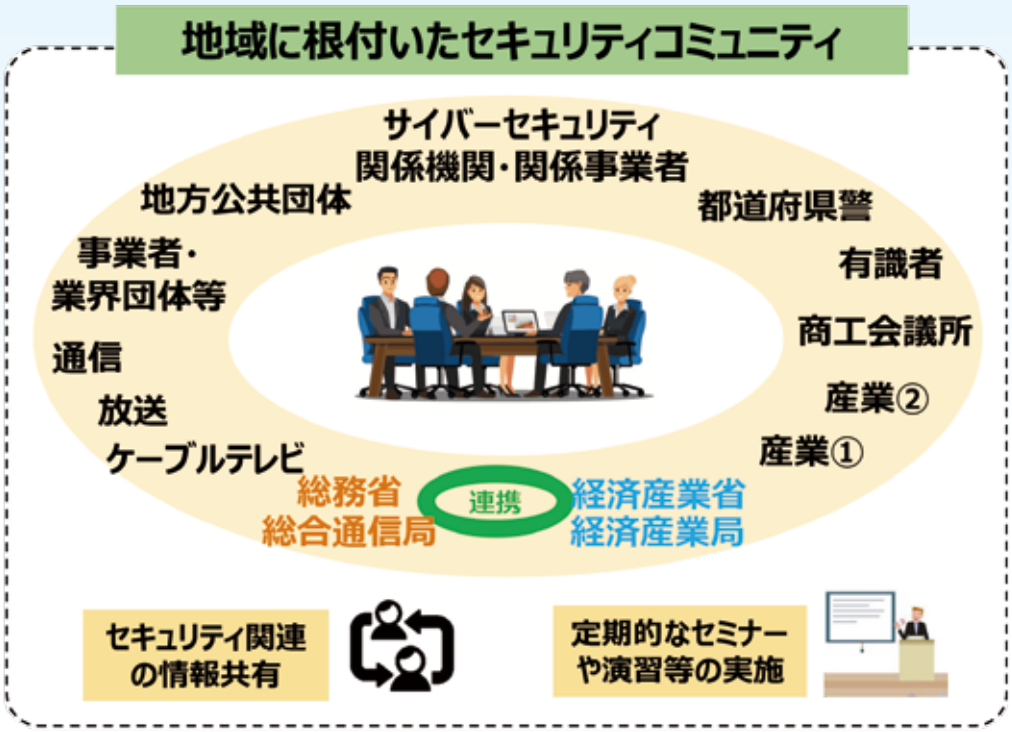
情報セキュリティに関する政府戦略である「第1次情報セキュリティ基本計画」が平成18年2月2日に策定されたことから、2月2日を「情報セキュリティの日」とし、平成22年からは2月を「情報セキュリティ月間」と定めました。その後、平成26年にサイバーセキュリティ基本法が成立したことを踏まえ、平成27年から期間を3月18日（サ（3）イ（1）バ（8）ーの日）まで拡大した上で、名称も「サイバーセキュリティ月間」と改め、内閣官房内閣サイバーセキュリティセンター（NISC）を中心として、サイバーセキュリティの普及啓発を集中的に実施しています。

地域SECUNITY（セキュニティ）強化に向けた総務省の取組

総務省では、地域のセキュリティコミュニティ（SECUNITY）（図1）の活動支援を通じ、地域におけるセキュリティ人材の育成や地域企業のセキュリティ強化を図っています。

この「サイバーセキュリティ月間」中にも、各地域で関連イベントを開催しますので、詳しくは総務省ホームページをご覧ください（参考）。

［図　1］



［参考］

【サイバーセキュリティ月間中のイベント等】

インシデント対応演習

最近のサイバーセキュリティインシデントの発生状況や、被害拡大を最小限にとどめるための基本的事項を説明し、擬似的なインシデント発生時対応手順を体験することにより、サイバー攻撃に対する組織内の基本方針やルールなどを考えていただくことを目的として開催しています。

若年層向けCTF

学生を対象としてサイバーセキュリティへの興味・意識を高めていただくことを目的とするCTF（Capture The Flagの略で、ゲーム形式でセキュリティの実践的技能を競うコンテストのこと）を開催しています。

地域 SECUNITY におけるイベント

管区	イベント名	開催期間
セミナー等		
北海道	サイバーセキュリティセミナー（名称未定）	令和5年2月9日
北海道	サイバーセキュリティセミナー（名称未定）	令和5年3月10日
北陸	サイバーセキュリティデイズ 2023（仮）	令和5年3月予定
東海	サイバーセキュリティセミナー 2023	令和5年3月10日
近畿	情報セキュリティセミナー in 大阪	令和5年3月17日
中国	中国地域サイバーセキュリティ連絡会交流セミナー	令和5年2月15日
九州	サイバーセキュリティカレッジ	令和5年2月8日
沖縄	サイバーセキュリティ月間セミナー in 沖縄	令和5年2月1日
サイバーインシデント対応演習		
北陸	サイバーインシデント演習	令和5年2月8日
関東	サイバーインシデント演習	令和5年2月14日
近畿	サイバーインシデント演習	令和5年2月21日
四国	サイバーインシデント演習	令和5年2月20日
若年層向け CTF		
東北	CTF ワークショップ in 仙台	令和5年2月4日

【参考 Web ページ】
イベントの詳細や申込み方法等は以下のページをご覧ください
https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

脆弱なIoT機器の利用者への注意喚起

ご利用のプロバイダからお知らせが届く場合があります

総務省及び国立研究開発法人情報通信研究機構（NICT）は、インターネット・サービス・プロバイダ（ISP）等と連携し、インターネットに直接接続される機器に対して、脆弱なID・パスワードが設定されているなどによって、サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者へ注意喚起を行う取組である「NOTICE」プロジェクトを2019年2月から実施しています（図2）。

また、大規模サイバー攻撃観測網「NICTER」により得られた情報をもとに、マルウェア（不正ソフトウェア）に感染していると検知された機器を特定し、その利用者に対して注意喚起を行う取組も、2019年6月から実施しています。

［図 2］

※NOTICE:National Operation Towards IoT Clean Environment

お知らせが届いた場合は

NOTICEサポートセンターにお問合せください。適切なセキュリティ対策を案内します。

なお、ご契約のISP以外から電話、訪問、費用請求、パスワードを聞き出すことはありません。

インターネット接続機器の設定をこの機に見直してみましょう

設定が十分でないと、不正アクセスを受けるおそれもあります。無線LANルーター等のインターネット接続機器について、次のポイントをチェックしましょう。

- **機器設定用のパスワードは複雑なものにしましょう。**
- **機器のファームウェアを最新の状態にしましょう。**

また、サポート期限が切れた機器はファームウェアの更新を適切に行うことができない場合がありますので、新しい機器に買い替えることも有効です。最新の無線LANルーターなどは、ファームウェア更新を自動で行うなどセキュリティ対策が行われているものもありますので、購入の際の参考にしてください。

お問い合わせ先

NOTICE サポートセンター

TEL：0120-769-318（無料・固定電話のみ）
03-4346-3318（有料）
受付時間：10:00 ～ 18:00
（年末年始（12/29～1/3）を除く）
URL：https://notice.go.jp
（NICTER に関する取組は https://notice.go.jp/nicter）

サイバーセキュリティ人材の育成

サイバー攻撃の悪質化・巧妙化が進む一方で、我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、その育成が喫緊の課題となっています。NICTのナショナルサイバートレーニングセンターでは、NICTがこれまでの研究開発で培った知見を活用して、サイバー攻撃に対する一連の対処を実際に体験する「実践的サイバー防御演習（CYDER）」を、国の機関や地方公共団体向けに実施中です。これまで6年間の受講者数は延べ1万6千人を超え、組織のインシデント対処能力の向上に貢献しています。

CYDER 演習風景

サイダコくん

CYDER 公式サイト
演習の詳細や受講申込はこちら
https://cyder.nict.go.jp/

Wi-Fiセキュリティ対策の推進

公衆Wi-Fiや自宅設置のWi-Fiは便利ですが、適切なセキュリティ対策を講じないと、情報漏えい等の被害につながってしまいます。このため、総務省では、Wi-Fiの安全な利用・提供のために必要なセキュリティ対策をわかりやすく解説したガイドラインを作成・公表していますので、是非参照してください。また、サイバーセキュリティ月間中に、ガイドラインのポイントをアニメや講義形式で解説したオンライン動画講座を開講予定ですので、こちらも是非受講してください。

総務省が作成・公表しているWi-Fiセキュリティガイドライン

ガイドラインの入手はこちら
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

テレワークセキュリティ対策の推進

テレワークは、時間や場所を有効に使い柔軟な働き方を可能とするものです。近年、働き方改革の実現や非常時の業務継続性確保といった観点から、その重要性は一層高まり、急速に普及が進んでいますが、テレワークに伴うセキュリティ上の不備を狙ったサイバー攻撃も増加しています。こうした状況に対応すべく、総務省では、テレワークを安全に実施するための「テレワークセキュリティガイドライン」と「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」を作成・公表していますので、是非活用してください。

総務省が作成・公表しているテレワークセキュリティガイドライン等

ガイドラインの入手はこちら
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/