【ニュースリリース】

2025 年 6 月 9 日
株式会社サイバーセキュリティクラウド

報道関係者各位

世界 2 位の“サイバー災害大国”日本に新たな備えを
サイバーセキュリティクラウド、「サイバー防災の日」に
企業・家庭それぞれに向けて『サイバー防災セット』を公開

株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、「6（ロッ）9（ク）の日」である、6 月 9 日（月）の「サイバー防災の日（※1）」にあわせて、企業・消費者それぞれに向け、常に自身が被害者になる可能性を秘めているサイバー攻撃に対して備えるための基礎的な内容をまとめた「サイバー防災セット（※2）」を公開いたします。

■背景・企画内容

現在、サイバー攻撃の発生件数は世界的に増加傾向にあり、サイバーセキュリティの重要性は一層高まっています。なかでも日本は、国別の標的件数で世界第２位に位置しており（※3）、多くの組織・個人がサイバー攻撃のリスクに晒されています。

特に近年、十分なセキュリティ対策を行っている大企業においても、ランサムウェアや標的型攻撃による被害が相次いでおり、業務停止や顧客情報の漏洩、株価への影響など、経営に直結する深刻な被害が発生しています。こうした被害は、企業活動の継続性や社会的信頼に重大な影響を及ぼすものです。
また、個人や家庭においても、フィッシング詐欺によるアカウント乗っ取りや不正送金、SNS を通じた情報の不正取得など、“サイバー災害”が拡大しています。これらの被害は、金銭的損失にとどまらず、プライバシーや安全性にも大きな影響を及ぼす可能性があります。

サイバー攻撃が常態化しつつある現在、サイバー攻撃対策の考え方も、「完全に防ぐ」から「攻撃を受けることを前提に、事前に備える」へと変化しています。

こうした背景から当社では、「誰もがサイバー攻撃の被害者になりうる」という認識を広め、少しでも多くの方に“サイバー防災”という発想を持っていただくことを目的に、6 月 9 日の「サイバー防災の日」にあわせて、企業および家庭がサイバー攻撃への備えとして実施すべき基本的な対策をまとめた「サイバー防災セット」を作成しました。本セットは、一般的な「防災セット」のように“サイバー災害”が身近に起きるという前提で、被害の抑制や早期対応を実現するために必要な最低限の取り組みを体系的に整理したものです。企業・個人の双方にとって実用的な指針となることを目指しています。

「サイバー防災セット」のリストは、防災セットのように、オフィスやご自宅の見えるところに用意して、常に“サイバー災害”時の初動を意識しましょう。
▶サイバー防災セットのダウンロードはこちら

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■「企業向け・サイバー防災セット」に関して

「企業向け・サイバー防災セット」は、「復旧戦略」「データ管理」「外部連携」「教育・訓練」「組織体制」の５つで構成された基本対策となっています。

★「筆が基礎（ふでがきそ）」で思い出そう！

ふ・復旧戦略：報告テンプレート・優先復旧システムの策定、信頼回復戦略
サイバー攻撃時の報告・開示テンプレートの用意、顧客・株主・メディアへの発信内容・タイミングの指針の策定、重要システムの復旧優先順位の明確化、代替手段やシステムの事前検討、再発防止に向けた分析体制と責任者の明確化など。

で・データ管理：定期バックアップ、フォレンジック対応環境の整備
重要システム・データの定期的なバックアップ、バックアップデータの隔離保管、ログの収集・可視化・保管体制の整備、フォレンジック調査に対応可能なツール・環境の用意など。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

が・外部連携：行政・警察・セキュリティベンダーとの連絡ルート確保
セキュリティベンダーやクラウドベンダーとの緊急対応連携体制の構築、IPA や警察、通信事業者等への通報フローの整備、顧問弁護士・法務部門との相談ルートの確保、委託先のセキュリティ水準と責任範囲の確認など。

き・教育・訓練：フィッシング訓練や復旧演習の実施と改善サイクルの確立
年 1 回以上のインシデント対応訓練の実施、フィッシングメールや標的型攻撃の模擬訓練の実施、復旧訓練や BCP 訓練の部門横断での実施、教訓の振り返りとマニュアルや教育内容への反映など。

そ・組織体制：指揮系統・マニュアル・緊急連絡網の可視化
サイバーインシデント対応フローの明文化や、CSIRT の設置、経営層・情報システム部門・広報部門の連携体制の確保、緊急連絡網の定期的な更新、初動対応マニュアルの作成と共有など。

■「家庭向け・サイバー防災セット」に関して
「家庭向け・サイバー防災セット」は、「パスワード・認証」「フィッシング」「SNS 炎上」「アカウント管理」「通知設定」の 5 つで構成された基本対策となっています。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

★「パフェ熱っ（ぱふえあつ）」で思い出そう！

ぱ・パスワード・認証：2 要素認証とパスワードマネージャーの活用
SNS やクラウドサービスのログインには 2 要素認証（MFA）を設定する。パスワードマネージャーを活用して複雑でランダムなパスワードを使用し、「自分で考えたパスワード」が過去に流出しているケースが多いため、リスト攻撃に備える。

ふ・フィッシング対策：不審リンクを“開かない”習慣
不審な SMS・メールのリンクや添付ファイルを開かない。多くの攻撃はフィッシングから始まり、1 クリックでウイルス感染や情報漏洩につながる危険性があります。

え・SNS 炎上：投稿内容に注意し“デジタルマナー”を意識
投稿前に「この内容が会社・学校・親に見られても問題ないか？」を確認する。写真に写り込んだ風景や制服、ナンバープレートなどから自宅や通学先が特定されるケースもあり、ストーカー被害や空き巣、詐欺に繋がるリスクがあります。

あ・アカウント管理：家族との使い回しによる想定外トラブルを防止
家族とのアカウント共有を避ける。ストリーミングやゲームなどのアカウントを子どもと共有すると、意図しない設定変更や課金トラブルが起きやすく、責任の所在が不明確になる危険があります。
また、OS やアプリを最新の状態に保ってください。古いままのシステムには既知の脆弱性が残っており、攻撃者にとって格好の標的となります。

つ・通知設定：クレカ利用・パスワード変更の即時通知で被害を早期発見
クレジットカード利用・ログイン・パスワード変更などに関する通知機能を有効化する。不正利用や乗っ取りにいち早く気づくことができ、被害を最小限に抑えられます。

【企業向け・家庭向けサイバー防災セットのダウンロードはこちら】
サイバー防災セットは、オフィスやご自宅の見えるところに用意して、常に“サイバー災害”時の初動を意識しましょう。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

※1 「サイバー防災の日」は、LINE 株式会社が制定した記念日であり、日付は「6（ロッ）9（ク）」の語呂合わせから、インターネット上でも防犯意識を持つ（鍵をロックする）必要があることを啓発する日とされています。
※2 「サイバー防災セット」は、サイバー攻撃に備えるための基本的な対策を厳選して整理したものです。これだけで万全というわけではなく、状況に応じた追加対策も重要となります。
※3 引用元：BlackBerry Japan 株式会社
https://www.blackberry.com/us/en/regions/ja/newsroom/press-releases/2024/blackberry-releases-global-threat-intelligence-report-for-q1-2024

■株式会社サイバーセキュリティクラウドについて

会社名：株式会社サイバーセキュリティクラウド
所在地：〒141-0021 東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
代表者：代表取締役社長 兼 CEO 小池敏弘
設立：2010 年 8 月
URL：https://www.cscloud.co.jp
「世界中の人々が安心安全に使えるサイバー空間を創造する」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使した Web アプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの 1 つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp