グローバル暗号デー

以下は、Global Encryption Coalition による「グローバル暗号デー」の趣旨説明の抄訳です。

グローバル暗号デー

現在、インターネットは脅威にさらされています。一部の国では、政府が強力な暗号化の使用を弱体化させるための新しいユニークな方法を見つけています。また、オンライン・セキュリティのベスト・プラクティスとしての暗号化を十分に活用していない国もあります。
暗号化は、秘密やプライバシーのためではなく、最終的には安全のためのものです。データの暗号化は何千年も前から行われてきました。古代エジプト人、メソポタミア人、スパルタ人、ローマ人は皆、セキュリティを確保するために何らかの形でコード化されたメッセージを隠していました。スマートフォンやコンピュータの普及に伴い、かつては一部の人だけが利用していた暗号化も、やがて誰もが利用できるようになるでしょう。暗号化によって、私たちは世界のどこからでも医療などの重要な機密サービスにアクセスできるようになります。暗号化によって、私たちは家族のプライベートな時間を共有することができます。内部告発者は恐れずに権力者に責任を問うことができ、変革を求める活動家は自信を持ってコミュニケーションをとることができます。
事実は私たちの味方です。暗号化は、私たちの医療記録の機密性を確保し、犯罪者から私たちを守り、ジャーナリストが権力者に説明責任を果たすことを可能にするなど、すべての人の安全を守ります。
しかし、エンドツーエンドの暗号化を守るためには、私たち全員が協力する必要があります。暗号化への取り組みの一環として、私たちは Global Encryption Coalition（世界暗号化連合）を支援し、強力な暗号化が私たちの生活にもたらす恩恵を皆で祝う機会を計画しています。Global Encryption Ðay」です。

しかし、この日を成功させるためには、世界中の専門家が必要です。私たちは以下のことを行います。

■強力な暗号化の使用を促進し、政府や法執行機関が暗号化を弱体化させようとする危険な試みを阻止するために、互いの努力を強化できるパートナーのグローバルな動きを構築する。
■エンド・ツー・エンドで暗号化されたサービスの価値を広め、ユーザーに「スイッチ」を促します。
■暗号化とエンド・ツー・エンドの暗号化サービスを支持するように世論を誘導する。
■グローバル暗号化連合に参加する戦略的メンバー（組織や企業）を募集する。
■ターゲット国で暗号化支持者のクリティカルマスを構築し、暗号化への脅威を撃退するための支持者に変える。
■グローバル・エンクリプション・デーにエンド・ツー・エンドの暗号化を行うことを企業に奨励する。
自分たちが信じるインターネットを擁護し、世界中のインターネットに関する意思決定において自分たちの立場を強化するためには、コミュニティ全体を惹きつけ、惹きつけ、強化することで、人々に力を与える必要があります。
Internet Society のメンバーは、論文やビデオの作成から、イベントの開催、国内のアドボカシーキャンペーンの主導まで、国内、地域、国際レベルで暗号化を支持しています。(以下略)

暗号化の仕組み

以下は、Global Encryption Coallition のウエッブに掲載されている暗号についての簡単な説明です。暗号は、インターネットの通信のプライバシーやセキュリティや相互の信頼性を高める上で必須の手段です。他方で、以下の説明にあるように、暗号を人々のセキュリティに用いる場合と国家のセキュリティに用いる場合とでは、場合によっては利害が相反することが起きます。近年の傾向として、政府等が人々の通信を監視する必要から、人々の利用する暗号(とくにエンド・ツー・エンド暗号)を弱体化させて、政府に暗号解読の特権を与えられるような法制度などの導入が試みられるようになっています。JCA-NET は、人々の暗号利用を弱体化させるいかなる法制度や政策にも反対する立場をとっています。

暗号化の仕組み

●暗号化とは何ですか？
暗号化とは、データをスクランブルまたはエンコードして、元の状態に戻す手段を持つ人だけが読めるようにするプロセスです。暗号化は、安全で信頼できるインターネットの重要な機能であり、機密情報のデータセキュリティを提供します。
●暗号化はどのような場合に使われるのですか？
暗号化は、コンピュータシステムに保存されているデータや、インターネットを含むコンピュータネットワークを介して送信されるデータを保護するためによく使われます。金融取引や個人的なメッセージのやり取りでは、セキュリティを高めるために暗号化がよく使われます。暗号化は、データが改ざんされていないかどうかを確認したり（データの完全性）、通信している相手が本当の相手であるという信頼性を高めたり（認証）、メッセージが送受信されたことを確認したりする際に重要です。
●暗号化の仕組み
ネットワーク上で通信されるデータの場合、最新の暗号化は、受信者と送信者だけが知っている秘密の値または鍵を使用してデータをスクランブルします。保存されているデータの場合、秘密の値は通常、データの所有者のみが知っています。暗号化にはさまざまな種類があり、最適なシステムでは安全性と効率性のバランスがとれるものになります。
エンド・ツー・エンドの暗号化は、最も安全な暗号化の形態です。(リンク先は英語)エンド・ツー・エンドの暗号化とは、送信者と受信者だけがメッセージを読むことができる暗号化方式のことです。通信サービスを提供している第三者であっても、暗号化キーを知ることはできません。
●暗号化が重要な理由
個人のセキュリティ
インターネットを利用した犯罪は、最も急速に増加しているセキュリティ上の脅威の一つであるため、暗号化はこれまで以上に重要な意味を持ちます。最も安全な暗号化方式であるエンド・ツー・エンドの暗号化により、何十億もの人々が毎日オンラインで送信する機密情報の機密性が保たれ、犯罪者の手に渡らないことが保証されます。
国家のセキュリティ
エンド・ツー・エンドの暗号化は、スパイ、テロリスト、敵対的な政府が、政府関係者の機密通信にアクセスして悪用したり、コンピュータシステムやデータベースに侵入して、経済、インフラ、セキュリティに大規模かつ体系的な混乱を引き起こすことを防ぎます。
また、法執行機関、軍関係者、機密業務を監督する政府関係者、緊急対応者の私的な機密通信も保護されます。また、暗号化は、電力網を動かすシステム、国民の機密データを含むデータベース、主権国家の経済的安定に不可欠な金融機関のデータベースなど、国家安全保障と本質的に結びついた機密性の高いシステムも保護します。

なぜ、暗号化は脅威にさらされているのか？

以下は、Global Encryption Coalition のサイトの記事の翻訳です。

なぜ、暗号化は脅威にさらされているのか？

暗号化はシステムです。システムの一部が弱体化すれば、システム全体が弱体化します。
一部の組織は、犯罪に対抗する手段として、暗号化を弱めようとしています。
これは、犯罪を防止するための努力を損なうだけでなく、何十億もの人々の個人的なセキュリティや、世界各国の国家安全保障を危険にさらす危険な前例を作ることになります。
一部の組織は、法執行機関に危険な権限を与え、犯罪撲滅のために企業に暗号化の「バックドア」の作成を義務付けるべきだと主張しています。
こうした主張は、企業のシステムやサービス上の暗号化された機密データへの、いわゆる「バックドア・アクセス」を認るものです。法執行機関に「バックドア・アクセス」を許可することは、何十億もの人々の個人情報や機密情報を公開し、犯罪者や敵対的行為者が悪用できる新たな危険なアクセスポイントを作り出し、犯罪防止のための努力を損なう危険で意図しない結果をもたらすでしょう。
バックドア・アクセスは、しばしば誤解を招く「例外的なアクセス」と呼ばれています。しかし、バックドア・アクセスには例外的なものはありません。
どのようなアクセスメカニズムであれ、バックドアが存在すれば、法執行機関と悪意のあるアクターの両方に悪用される可能性があります。犯罪を防ぐために「バックドア・アクセス」を作って暗号化を弱めることは、1つの問題を解決するためにさらに1,000の問題を作ろうとするようなものです。暗号化の「バックドア」は、犯罪者やテロ組織などの敵対的な行為者を含め、誰でも見つけることができ、開けることができてしまうために、世界的に暗号化を弱める可能性のある危険な前例となります。
暗号化の使用が弱められたり制限されたりすると、私たち全員がより大きなリスクにさらされることになるのです。

グローバル・暗号デー・ステートメント – 2021年10月21日

強力な暗号化は、人々やその情報、通信の秘密と安全を守るための重要な技術です。オンラインでの信頼を支え、脆弱なコミュニティのメンバーを保護し、政府、企業、市民のデータを犯罪者やその他の悪意のあるアクターから守ることができます。
しかし、一部の政府や組織は、暗号化の弱体化を推進しています。これは、世界の何十億もの人々のセキュリティとプライバシーを危険にさらす、危険な前例となるでしょう。暗号化を弱体化させる一国の行動は、私たち全員を脅かします。
グローバル暗号デーに、私たちは、各国政府と民間企業に対し、暗号化を弱体化させようとする動きを拒否し、代わりに、世界中の人々を守るために強力な暗号化を強化、強化、使用を促進する政策を追求することを呼びかけます。また、企業が自社のサービスやプラットフォームに強力な暗号を導入して顧客を保護しようとする努力を支持、奨励します。
強力な暗号化は、私たち全員にとって、より安全な世界を実現するための重要なツールです。
署名団体(省略)

10 月 26 日(火)JCA-NET セミナー　午後 7 時から

(テーマ) 市民運動・社会運動のための暗号入門(1)
使用するテキスト『反対派を防衛する：社会運動のデジタル弾圧と暗号による防御』(Glencora Borradaile 著)
開催方法　オンライン(参加方法は下記を参照)

10 月 30 日(土)JCA-NET セミナー　午後 3 時から

(テーマ) 市民運動・社会運動のための暗号入門(2)
使用するテキスト『反対派を防衛する：社会運動のデジタル弾圧と暗号による防御』(Glencora Borradaile 著)
開催方法　オンライン(参加方法は下記を参照)

オンラインでの参加方法

JCA-NET セミナーのオンライン参加方法について
参加費：無料(カンパ歓迎です)
オンラインは Jitsi-meet を使用します
参加方法：JCA-NET の会員メーリングリスト、セミナーメーリングリストに登録されている方は、当日 30 分前に、メーリングリストからの会議室案内をみてアクセスしてください。
JCA-NET の会員以外の方でセミナーに初めて参加される方は予約が必要です。おなまえ、メールアドレス、参加希望のセミナー番号(複数可)を書いて、下記に申し込んでください。
jcanet-seminar@jca.apc.org
問い合わせ先
小倉利丸(JCA-NET 理事)
toshi@jca.apc.org
070-5553-5495
Jitsi-meet のマニュアル
https://www.jca.apc.org/jca-net/ja/node/93