

暗号：私達のプライバシーとセキュリティへの鍵

2022 年 10 月
グローバル暗号化デー用

強力な暗号化は、私たちがオンラインでもオフラインでも安全であり続けるための基本的な要素です。誰もメッセージを盗み聞きしたり、改ざんしたりしないという確信のもと、人々は安全に他者とコミュニケーションをとることができるのです。

にもかかわらず、世界中の政府はエンド・ツー・エンド暗号化（E2EE）に対する攻撃を強化しています。政府は、E2EE を法執行機関の障害とみなしているのです。しかし、人々のデジタル・セーフティを組織的に弱体化させることは、解決策にはなりません。

エンドツーエンドの暗号化は、日常生活のオンライン化が進む世界において、セキュリティのゴールドスタンダードです。私たちは、E2EE を弱体化させようとする政府の取り組みに反撃する必要があります。

グローバル暗号化デーには、エンドツーエンド暗号化を保護し、それを弱体化させるいかなる提案も打ち負かすための私たちの取り組みに参加するよう、皆さんに求めています。私たちはすでに、エンドツーエンド暗号化にバックドアを設けようとする試みがいかに支持されないかを示しました。今、私たちは、各国政府が提案するその他の抜け道を阻止する必要があります。

出典： <https://www.jca.apc.org/jca-net/ja/node/227>

原文： <https://www.globalencryption.org/2022/06/global-encryption-day-2022/>

グローバル暗号化連合とグローバル暗号化デー

Global Encryption Coalition:

- 2020 年に設立。
- 現在、約 300 名の個人・組織会員。
- ウェブサイト: <https://www.globalencryption.org/>



Global Encryption Day:

- 目的: 私達の安全(プライバシーとセキュリティ)を守る要素である強力な暗号化を増進・保護すること。
- 日時: 2022 年 10 月 21 日(金); 2020 年から毎年。
- イベント一覧:
<https://www.globalencryption.org/events/ged/2022-events/>

暗号化とは？

暗号 (cryptography) :

- "cryptography" = "crypto" (隠れ、秘密) + "graphy" (術、科学)。
- 敵が存在する環境における安全な通信手法に関する学問と実践。
- 暗号化に加えて、署名、ハッシュ、匿名化なども範囲内。
- 基礎: 数学、計算科学、コード。

暗号化 (encryption) :

- 情報が読めないようにするプロセス。
 - 対義語: 復号化 (decryption)。
- "暗号化" は暗号 (cryptography) 全般を指す場合が少なくない。

今後、「暗号」という単語で指す。

暗号化の背景

冷戦時代:

- 暗号化は「軍需品」として指定され、輸出規制対象に。

暗号戦争 "Crypto Wars" (1990 年代):

- PGP 暗号のリリース (1991)、書籍として米国から輸出 (1995)。
- クリッパーチップ (バックドア) が NSA に開発 (1993)、消滅 (1996)。

スノーデン暴露 (2013):

- BULLRUN (NSA 暗号化弱体化プログラム) が明らかに。
- 暗号化の普及・再評価・強化をするきっかけとなった。

暗号戦争 2 (2014- 現在):

- アップルとグーグルが自身の製品の暗号化データへのアクセスを削除 (2014)、米政府が反発; アップル対 FBI 紛争 (2016)。
- 立法上の脅威: 英 Investigatory Powers 法 (2016)、豪 Assistance and Access 法 (2018)、米 EARN IT 法案 (2020- 現在)、など。

暗号化に対する現在と新興の脅威

暗号化利用者に対する懲罰:

- 鍵・パスワード引き渡しもしくは復号化の強要。
- 暗号化の輸出入・使用に関する規制。
- 人のデジタルデバイスに対する合法または違法のハッキング。
- 警察によるまたは水際でのデジタルデバイス搜索。

技術的障害:

- VPN・Torなどの利用者に対するウェブサービス提供拒否。
- プライバシーツールを提供するウェブサイトに対する検閲。
- 広範囲インターネット検閲やシャットダウン。

その他:

- テロ、過激主義、組織的犯罪、児童虐待などを暗号化のせいにするデマ・プロパガンダ。
- 法案: ChatControl (欧)、EARN IT 法案 (米)、LEAD 法案 (米) など。

現代社会における敵対環境

- インターネット監視がさまざまな者によって犯されている。
- カメラ、スマホや他のセンサーが蔓延している。
- 私達の人生のすべてが激しくデジタル化されている。
- 多くの行動や相互作用が永久に記録されている。
- 法律と規範が時間とともに変化;記録は増加しつつある脅威。
- 人間による判断がアルゴリズムに置き替えられている。
- 私達のデータがストーキングや利益などの恣意目的に悪用されている。
- 過去の情報流出、デジタル化や怠慢なセキュリティによって可能になっているフィッシングとサイバー攻撃が増えつつある。
- 平和的抗議、人権保護活動家、ジャーナリスト、内部告発者などが暴力的な組織によって頻繁に標的にされる。
- 権威主義的な手段はいわゆる「自由民主社会」に浸透している。

暗号の重要性

- 現代社会において、暗号は監視から私達および社会を保護し、デジタルシステムのセキュリティ強化に役立つ。
- 私達は、秘密性、匿名性、完全性と真正性を施行するための非暴力的かつ技術的なツールとして暗号を利用できる。
- 個人規模からコミュニティや社会までにおいて、ビジネス、民主主義、自由、プライバシー、安全と信頼を築くために暗号は極めて重要。
- 使用例：社会的支援、弁護士との秘密、医療の秘密、報道、恋愛関係、家族事、直接行動、ビジネス。

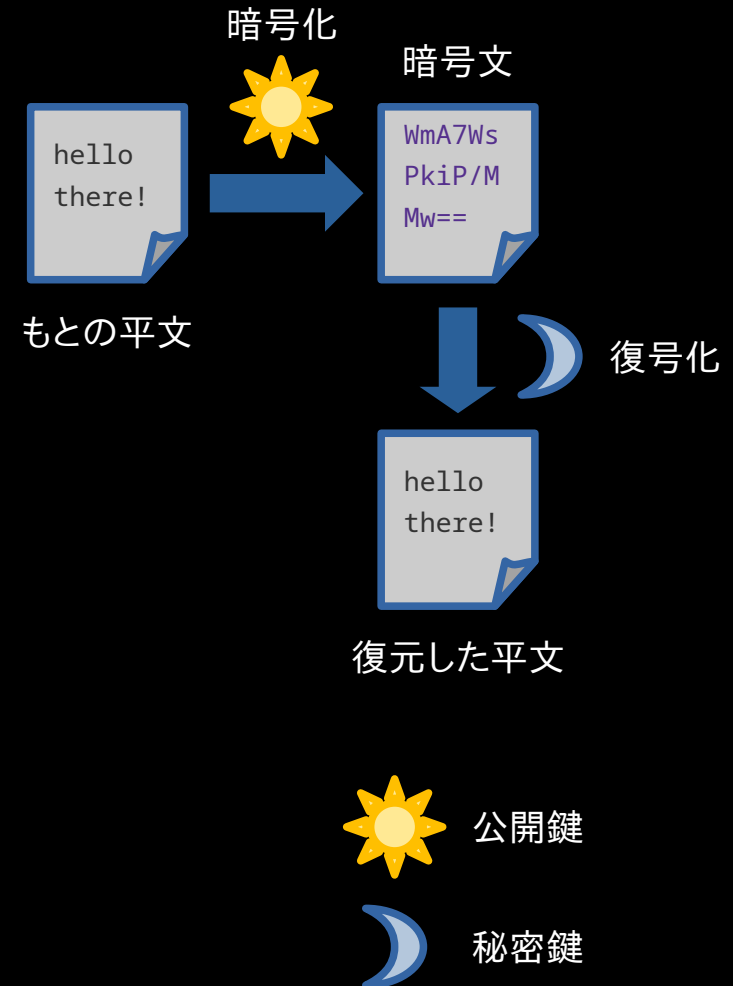
基本概念(1) — 暗号化

対称鍵暗号化 a.k.a. 秘密鍵暗号化:

- データを同じ共通鍵で暗号化・復号化。
- 暗号化・復号化の仕組みが素早い。
- 秘密の鍵・パスワードの安全共有が課題。

非対称鍵暗号化 a.k.a. 公開鍵暗号化:

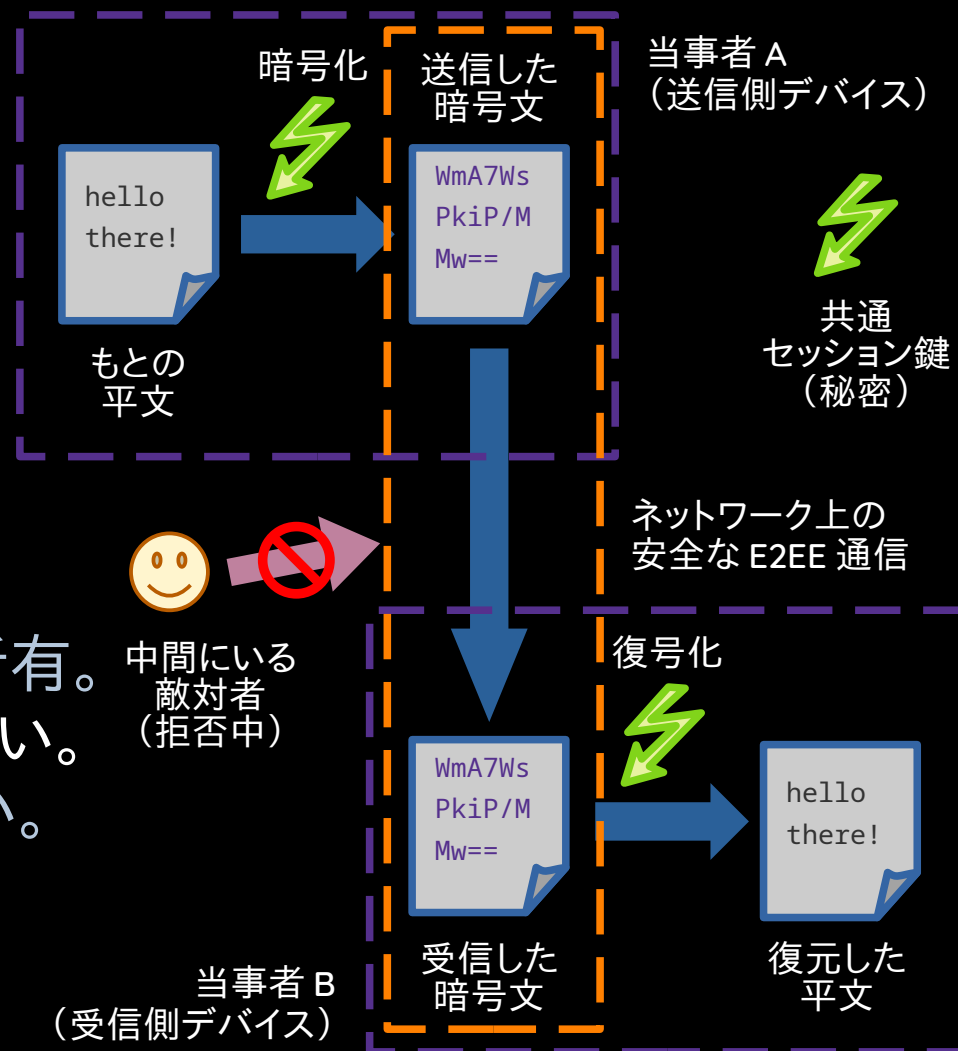
- 公開鍵で暗号化;秘密鍵で復号化。
- 公開鍵を安全に公開でき、簡単に共有可能。



基本概念(2) — エンド・ツー・エンド暗号化

エンド・ツー・エンド暗号化 (E2EE) :

- ほとんどは非対称と対称鍵暗号化を併合して実現。
- 普通は相手認証のための何らかの暗号手法も使われる。
- 当事者が自分の秘密鍵を排他的所有。
- 当事者以外の鍵が通信に関与しない。
- 中間者が通信を盗聴・操作できない。



基本概念(3) — 匿名性

匿名性:

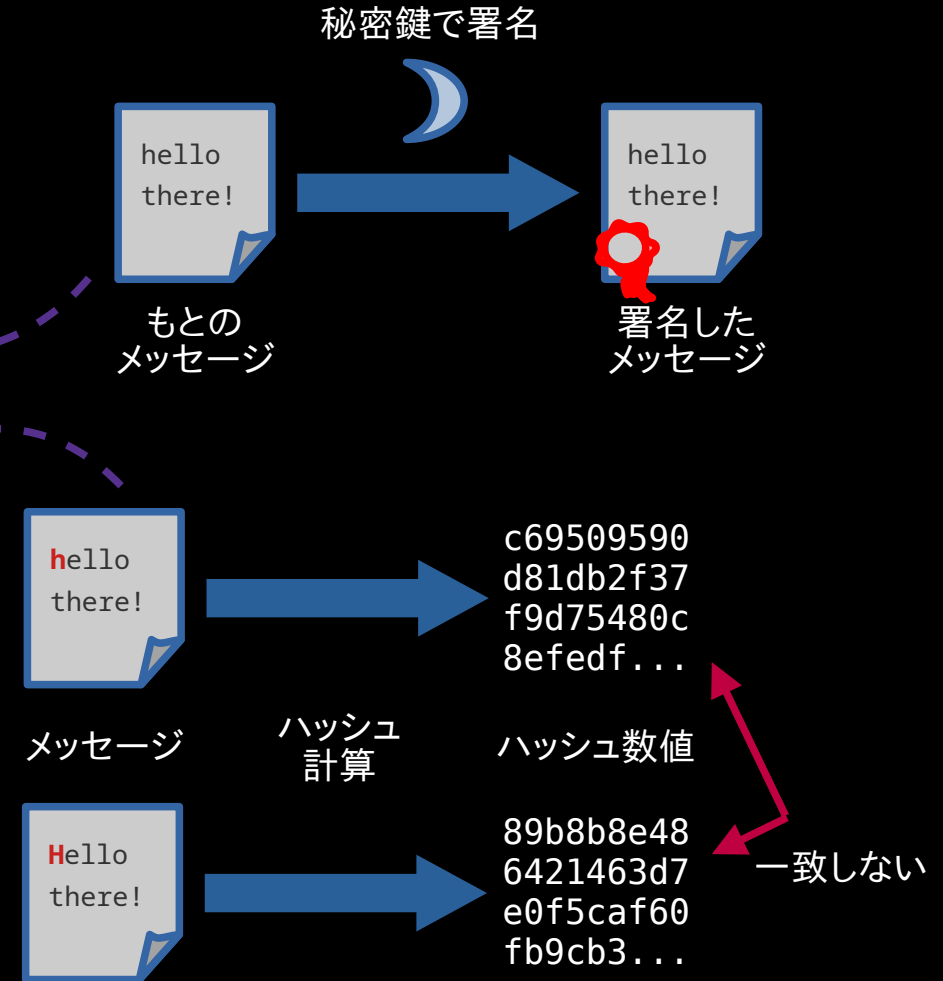
- 身元特定が不可能な状態。
- 秘密情報を保護する暗号化とよく対照。
- 匿名化の例:
 - 身元を特定し得る情報を作成しない。
 - インターネット通信の起点と行先を隠す。

仮名性:

- 実名に結ばれていない名称を使うこと。
- 匿名性より弱い保護; 一連の行動が仮名に結ばれることが可能。
- 匿名性と対照し、評判の蓄積を容易にする。

基本概念(4) — 暗号化だけではない

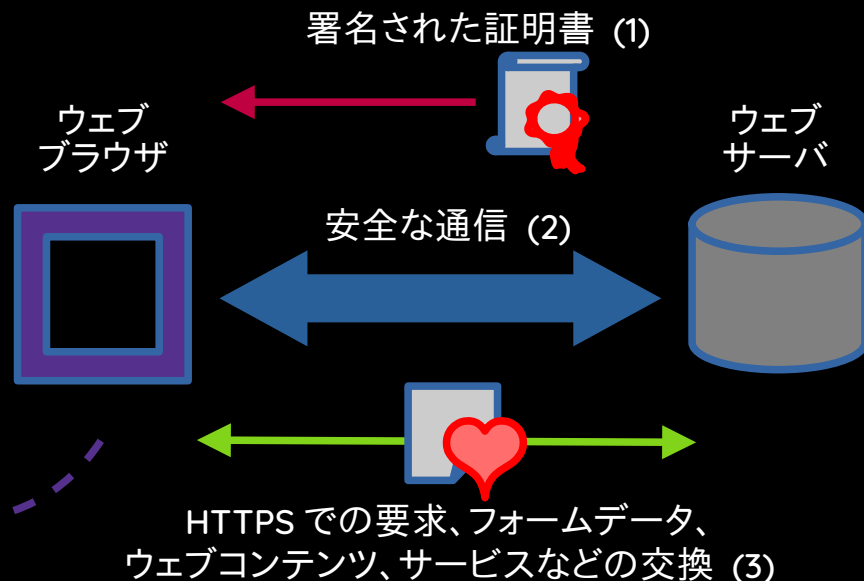
- **署名**: 秘密鍵を使って、データに対する完全性および真正性の証明をつくる。
- **ハッシュ**: データを数値に決定的に変換; 完全性検証に使われる。
- **ゼロ知識証明**: 立言の真偽以外の情報を開示せずに立言が真であることを証明。



応用(1) — ネットワーク通信暗号化

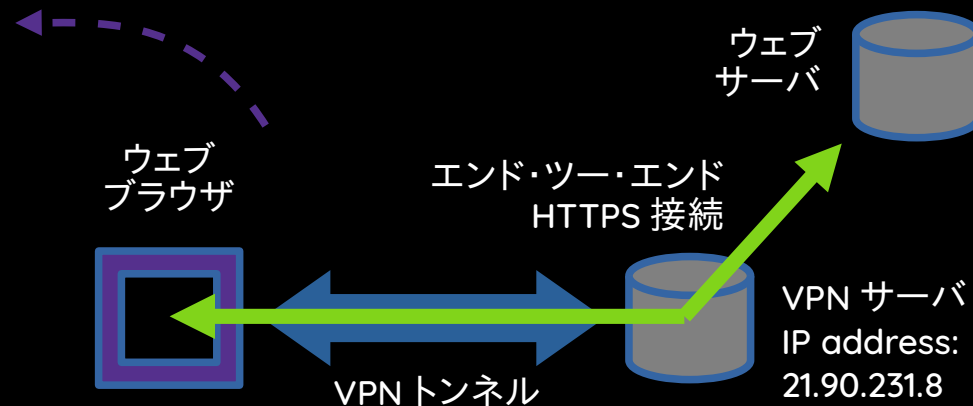
TLS (transport layer security):

- 対象: メール、ウェブ (HTTPS) など様々な通信。
- 証明書(公開鍵)でサーバ認証と共通鍵交換。



VPN (virtual private network):

- 分離しているネットワークの間に安全なトンネルをつくる。
- 検閲回避と弱い利用者 IP アドレス保護として多く使われる。



応用(2) — ネットワーク通信匿名化

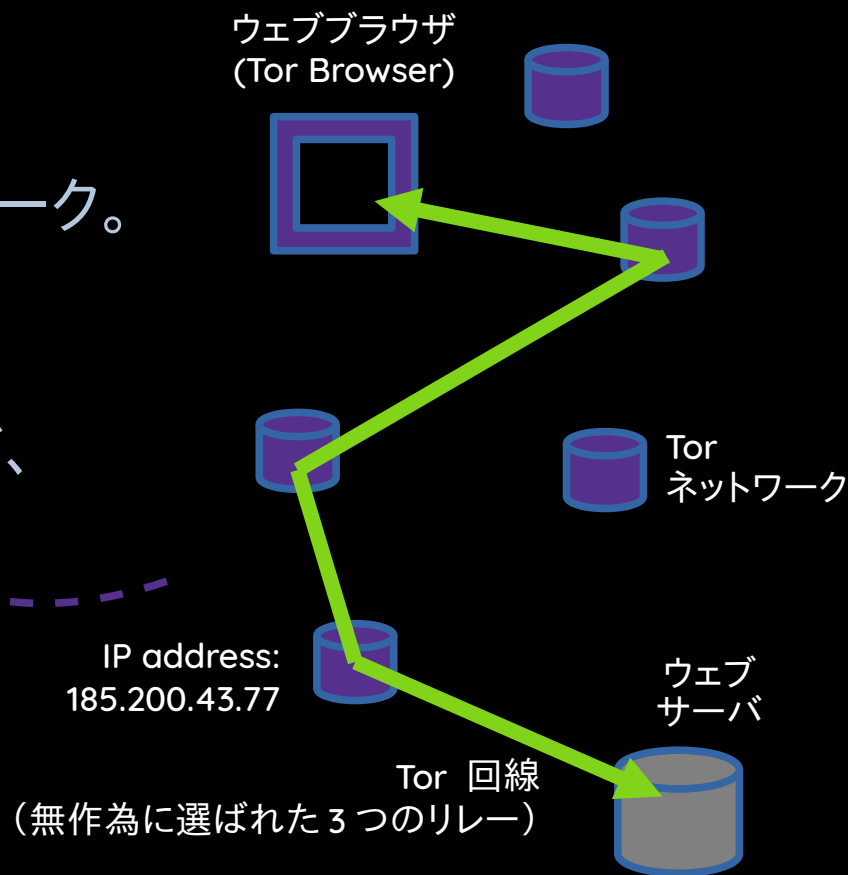
(より)匿名にインターネットを利用するために。

Tor: <https://torproject.org/>

- もっとも多く使われている匿名化ネットワーク。
- Tor Browser: 匿名性に特化した Firefox 型ウェブブラウザ。
- 使用例: ウェブブラウジング、ダウンロード、ファイル共有、メッセージャー、...

他のネットワーク:

- **I2P:** <https://geti2p.net/>
- **Lokinet:** <https://lokinet.org/>
- **Nym:** <https://nymtech.net/>



応用(3) — E2EE 安全通信

- **Briar** 回復力のある peer-to-peer チャット: <https://briarproject.org/>
- **Cwtch** Tor 経由非中央型チャット: <https://cwtch.im/>
- **Jami** SIP 型 peer-to-peer チャット: <https://jami.net/>
- **Jitsi** ビデオ通話: <https://jitsi.org/>  **peer-to-peer モードのみ E2EE**
- **OnionShare** ファイル共有とサイト発行: <https://onionshare.org/>
- **OpenPGP** ファイル・データとメールの暗号: <https://openpgp.org/>
- **Session** 非中央型チャット: <https://getsession.org/>
- **SSH** 遠隔シェルへの接続。
- **Signal** 中央型チャット: <https://signal.org/>  **電話番号が必要**

応用(4) — 他の暗号

静止時暗号化:

- Android と iOS のデバイス暗号化。
- **KeePassXC** PC 用パスワード管理: <https://keepassxc.org/>
- **KeePassDX** Android 用パスワード管理: <https://keepassdx.com/>
- **LUKS** ファイルシステム暗号化。
- **VeraCrypt** 暗号化ファイルシステム: <https://www.veracrypt.fr/en/>

署名と検証:

- **OpenPGP** ファイル・データとメールの暗号: <https://openpgp.org/>

ハッシュ計算:

- BSD、Cygwin、GNU/Linux、macOS と Termux
に含まれる **shasum**、**sha512sum**、**b2sum** など。
- **GtkHash** GUI ツール: <https://gtkhash.org/>
- **OpenSSL** コマンドラインツール: <https://www.openssl.org/>

暗号を利用時の最良実践(1)

一般:

- 良好な乱数源から生成した強力な無作為パスワードを使う。
- 暗号の使用に関する自分の地域の法的・政治状況を確認する。
- 暗号化が任意なソフトウェアに、暗号化が有効なことを確認する。
- 不正アクセスと悪質ソフトウェアから自分のデバイスを守る。

暗号のセキュリティ:

- 実績の良いライブラリ・アプリケーションを採用し、安全に設定する。
- 脆弱または危険かもしれないアルゴリズム・モードを拒否する:
 - 楕円曲線暗号: brainpool、NIST、secp256k1、...
 - 対称鍵暗号化: 3DES、RC4、XOR cipher、...
 - 乱数生成: Dual_EC_DRBG。

暗号を利用時の最良実践(2)

鍵:

- 通信を信用する前に相手認証を行う。
- 誰にも自分の秘密鍵を渡さない。
- 自分の秘密鍵が不正入手または流出されたと疑う場合、新しい秘密鍵に移行して連絡先にそれを通知する。

ソフトウェア:

- 実績の良い自由オープンソースソフトウェア (FOSS) を使う。
- ソフトウェアを採用する前に、機能、使いやすさ、要件、開発状況と適性を確認する。
- 公式入手先からソフトウェアを安全にダウンロード、検証と定期更新をする。

行動の呼びかけ

文化:

- プライバシー、匿名性、同意と情報セキュリティを正常化する。
- 自分のグループやコミュニティにおいて暗号の使用を奨励する。

政治:

- 監視賛成、反プライバシー、反匿名性または反暗号化のプロパガンダ・政策を拒否して反撃する。
- 暗号が私達を力づけて社会を保護してくれることを強調する。

技術:

- できるだけ頻繁に広範囲にわたって暗号を使う。
- 寄付、コード、テスト・バグ報告、翻訳、文書化やサービス提供などでFOSS 暗号プロジェクトを支援する。

リンクと資料

グローバル暗号化連合 (Global Encryption Coalition)

<https://www.globalencryption.org/>

動画: <https://www.youtube.com/channel/UCMh32OaTNU2P5CtOk0l8V8Q>

グローバル暗号化デー 2022 イベント (Global Encryption Day)

<https://www.globalencryption.org/events/ged/2022-events/>

Electronic Frontier Foundation, *Surveillance Self-Defense*

<https://ssd.eff.org/>

Eric Hughes (1993), *A Cypherpunk's Manifesto*

<https://www.activism.net/cypherpunk/manifesto.html>

ここからも入手: https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto

グレンコラ・ボラダイル著、小倉利丸 訳『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』、2021 年

[https://www.jca.apc.org/jca-net/sites/default/files/2021-11/ 反対派を防衛する \(統合版 \).pdf](https://www.jca.apc.org/jca-net/sites/default/files/2021-11/反対派を防衛する(統合版).pdf)

関連記事: <https://blog.torproject.org/book-defend-dissent-with-tor/>



CC0. No rights reserved.

注意事項:

- この資料は手短い概要で、完全ないし正確ではない。
- この資料内の特定のソフトウェア・資料への言及は推奨であるわけではない。
- 特にソフトウェアを入手する際、この資料内のリンクを確認してから使用すること。