1st Edition

Defend Dissent

Digital Suppression and Cryptographic Defense of Social Movements

Glencora Borradaile

Open Educational Resources

Oregon State University

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

グレンコラ・ボラダイル

目次

訳者まえがき....6
はじめに なぜデジタルセキュリティなのか？ -- 反監視情報....7
はじめに なぜデジタルセキュリティなのか？....7
「安全」なアプリをダウンロードするだけでは不十分....7
この本の政治的範囲....8
この本の概要....8
第 1 部 暗号技術の紹介....8
第 2 部：デジタルによる社会運動の弾圧 (米国の場合)....9
第 3 部：社会運動を守るために (アメリカ編)....9
次章で学ぶこと....9
Part1:暗号技術入門....11
暗号化とは何か？....11
シンプルな暗号。シーザー暗号....11
少しだけ複雑な暗号。ヴィジュネル暗号....12
コンテクスト：破れないワンタイムパッド....12
次に学ぶべきこと....13
図版の出典....13
現代の暗号技術....13
ブルートフォース・アタックを必要とするセキュリティ....13
隠匿では安全性を確保できない....14
透明性がもたらすセキュリティ....14
暗号化キーの保護によるセキュリティの確保....16
インフラへの不信感がセキュリティにつながる....16
コンテクスト：エニグマ・マシン....18
次に学ぶこと....19
図版の出典....19
暗号化のための鍵の交換....19
物理的な例。鍵を交換せずにメッセージを交換する場合....19
数学的な例。鍵を交換せずにメッセージを交換する方法....20
物理的な例。安全でないチャンネルでの秘密の合意....21
ディフィー・ヘルマン鍵交換(Diffie-Hellman Key Exchange)....23
ディフィー・ヘルマン鍵交換の利用....24
コンテクスト： 良いことが悪いことに....25
次に学ぶべきこと....25
外部リソース....25
図版の出典....25
暗号化ハッシュ....25
自分の頭の良さを証明する暗号化ハッシュ関数の使い方....26
ハッシュ関数はどのようなものか？....26
コンテクスト： 暗号化ハッシュは憲法修正第 4 条の権利を侵害する....27
次に学ぶべきこと....28
外部リソース....28
中間者....28
物理的な中間者攻撃....29
ディフィー・ヘルマン鍵交換に対する中間者攻撃....31
暗号ハッシュによる中間者攻撃の発見 フィンガープリンティング....32
帯域内フィンガープリンティング....33
フィンガープリント認証は、全員がやらなくても保護になる....35
フィンガープリントができないときの対処法....35
コンテクスト：中国のグレート・ファイア・ウォール....35
次に学ぶこと....36
外部リソース....36
図版の出典....36
パスワードについて....36
「パスワード保護」が暗号化を意味しない場合....36
パスワードのクラッキング....37
パスワードのベストプラクティス....38
パスワードから暗号化キーを生成する....39
コンテクスト： 対策が破られるとき....40
次に学ぶこと....40

外部リソース....40
図版の出典....41
公開鍵暗号方式....41
ディフィー・ヘルマン鍵交換の再検討。公開鍵暗号方式か対称鍵暗号方式か？....42
公開鍵暗号方式と対称鍵暗号方式の組み合わせ....43
コンテクスト 反核活動と Pretty Good Privacy....44
次に学ぶこと....45
外部リソース....45
図版の出典....45
暗号化された署名による真正性(authenticity)....45
暗号化ハッシュへのデジタル署名....46
暗号化された署名の用途....47
ソフトウェアの検証....47
フィンガープリント認証と「信頼の輪」の管理....48
コンテクスト：令状のカナリア....48
次に学ぶこと....49
外部リソース....49
図版の出典....49
メタデータ....49
メタデータとは何か？....49
メタデータとインターネット....50
コンテクスト： 内部告発者の保護....51
次に学ぶこと....51
外部リソース....51
匿名ルーティング....52
中間者を信じて使う：仮想プライベート・ネットワーク....53
中間者を信用しなくてよい：Onion Router (オニオン・ルーター)....54
匿名ブラウジング技術の利用とそれへの妨害....57
コンテクスト： Ðisruptj20....58
次に学ぶこと....58
外部リソース....58
図版の出典....59
Part2：社会運動へのデジタルな抑圧 社会運動へのデジタルな抑圧（アメリカ編）....60
社会運動抑圧のメカニズム....60
抑圧の手口....60
1. 直接的な暴力....60
2. 法制度....61
3.雇用の剥奪....61
4.あからさまな監視....62
5.秘密の監視....62
6. 騙し....63
7.マスメディアの影響....63
情報技術による妨害....64
コンテクスト COINTELPRO の時代....64
1. 直接暴力....65
2. 法制度....65
3. 雇用の剥奪....66
4. 露骨な監視....66
5. 秘密裡の監視....66
6. 偽装....66
7.マスメディアの影響....67
次に学ぶこと....68
外部リソース....68
図版の著作権者....68
社会運動に対するデジタルの脅威....68
監視を仕掛けてくる敵対者....69
監視戦略....70
監視戦術....71
大規模な傍受とデータの収集....72
データの集約と分析....73
標的を狙ったデータ収集....73
デバイスへの攻撃....74
個人的な嫌がらせ....75

コンテクスト：スタンディングロック....76
次に学ぶこと....77
出典....77
図版の著作権者....78
Part3：反対運動を防衛する 社会運動を守るために（アメリカ編）– 反監視情報....79
監視と抑圧から身を守る....79
脅威を軽減すること....80
監視能力を低下させる....80
弾圧のリスクを減らす....80
データ取得にかかる労力を増やす....80
あなたのデータはどこに？....80
コンテクスト：エドワード・スノーデン....81
次に学ぶこと....82
外部リソース....82
出典....82
セキュリティ文化....82
セキュリティ文化とデジタル・セキュリティの接点....83
知る必要について：情報の共有とデジタル化を最小限に抑える....83
知るということ：交流と信頼の構築....83
ゴシップやうわさ話をしない....83
コンテクスト： セントポール原則....84
次に学ぶこと....84
外部リソース....84
デバイスを守る....85
実体的攻撃....85
どうすべきか？....86
リモート攻撃....87
何ができるのだろうか？....88
コンテクスト：デモ参加者の携帯電話を危険にさらす....88
次に学ぶこと....89
外部リソース....89
通信を守る....89
暗号化されているかどうか....90
データ転送中の暗号化....91
エンド・ツー・エンドの暗号化....92
認証....92
コンテクスト：多人数のビデオチャット....93
次に学ぶこと....93
外部リソース....94
図版の出典....94
リモートデータを守る....94
コンテクスト：暗号化とクラウドストレージへの信頼....95
次に学ぶこと....96
図版の著作権者....96
自分のアイデンティティを守るために....96
匿名と仮名....96
Tor の使用方法....97
自分の位置を隠す....97
匿名性の確保....97
仮名性の確立と維持....97
Tor の警告....98
コンテクスト：本物の Tor ブラウザを手に入れる....98
次に学ぶこと....98
結論 デジタルセキュリティツールの選択....99
必須の基準....99
追加の望ましい技術的基準....100
技術以外の基準....101
Creative Commons License....102

訳者まえがき

本書は、Glencora Borradaile, Ðefend Ðissent, Ðigital Suppression and Cryptographic Ðefense of Social Movements (Oregon State University, 2021)の翻訳です。本書は、主に、社会運動に関わる人々を対象に、インターネット時代に急速に拡がりはじめている捜査機関による監視やネットへの取り締まりによる運動への弾圧に対抗するための基本となる考え方と、実践的な取り組みについて、週末や休日に読み切ることができる長さを念頭に置いて書かれたものです。

著者は、コンピュータサイエンスの専門家であると同時に、活動家でもあり、米国の活動家が大量監視と巧妙な監視技術によって日々直面しているリスクにを深刻に受けとめ、セキュリティの専門家ではない人達にも必要な最低限の知識と情報の提供を念頭に置いています。

本書の構成など詳細は、著者による冒頭の説明を参考にしていただくのが一番ですから、ここではごく簡単に、日本の読者の皆さんを念頭に、本書の意義について書いておきます。本書の特徴は、書名の副題にあるように、コンピュータ・コミュニーション領域で進展しつつある警察などによる弾圧技術の高度化を念頭に、高度化する弾圧への対抗手段の確保です。プロバイダーなどが保有するデータへのアクセスは頻繁に行なわれています。スマホやパソコンは押収されれば確実に内部のデータやクラウドのデータを取得されると考えなければならないでしょう。AI、生体認識技術、ビッグデータ利用が進むなかで、ネットワーク盗聴、ネットでの活動の追跡や行動予測が進歩し、私たちの体感では捕捉しづらい手法で私たちの基本的人権が侵害されています。こうしたなかで、本書は、私たちの防御の手段の核心に「暗号」を据えました。監視や盗聴から私たちのコミュニーションを防衛する最後の砦が暗号です。暗号技術を駆使することによって、私たちは、たとえ、デバイスが押収されたり盗聴・追跡されたり、契約しているプロバイダーが捜査機関に協力したりしても、データを解読することはでず、私たちの行動の監視を防御することも可能になります。内部告発者が告発の証拠をジャーナリストに渡す場合も、人権活動家が弾圧を回避して支援する場合も、暗号技術なしには、私たちのリスクを最小化することはできません。完璧とはいえないとしても、暗号は私たちのセキュリティにとって必須のものなのです。このことを本書は、技術の仕組みから現実の運動での活用まで、平易に説明しています。事例は米国のものですが、日本にも十分あてはまるものです。日本では社会運動の担い手たちが暗号の重要性を運動の文化にとっての共通認識にすることがますます必要になっています。この意味でも本書は重要な意味をもつと思います。

翻訳にあたって、コンピュータ技術に関連する用語の説明や暗号の仕組みや米国の国内事情などを補足しました。

翻訳は、JCA-NETの月例セミナーに参加してくださった方たちの協力を得ています。翻訳の最終的な責任は小倉にあります。

本書の著作権は、Creative Commonsのライセンスです。非営利での利用であれば自由に複製していただいてかまいません。(ライセンスの詳細は本書の最後に掲載してあります)

本書を使っての学習会などの開催も歓迎します。学習会などの相談にものります。また訳文などについてご意見やご提案、間違いの指摘などいただければ有り難いです。本書は下記からダウンロードできます。

https://www.jca.apc.org/jca-net/ja

2021年11月2日

小倉利丸 toshi@jca.apc.org

はじめに なぜデジタルセキュリティなのか？ – 反監視情報

はじめに なぜデジタルセキュリティなのか？

2013年夏、エドワード・スノーデンは、米国家安全保障局（NSA）、米中央情報局（CIA）をはじめとする世界各地の3文字機関から開示された大量の文書で世界を震撼させました。この1年以上の間、これらの機関のデジタル情報収集能力の高さ、特に米国の情報収集能力の高さが、毎日とは言わないまでも毎週のように明らかにされました。NSAは、インターネットや電話のネットワークを介して、暗号化されていないあらゆる情報に加え、弱い暗号化が施された情報や、企業のサーバーで暗号化されていない情報も入手できているように感じられました。その感覚は真実に近いものがあります。

当時、私は環境保護活動に従事しており、社会運動が歴史的にスパイ活動による国家弾圧に苦しめられてきたことを知っていました。NSAやCIAが収集できる情報の量が多ければ多いほど、国家による弾圧はより簡単で効果的なものになります。国家があなたの活動についての情報を知れば知るほど、あなたの目的を妨げることが容易になります。

だから、私は心配だったのです。気候変動に立ち向かうために活動しているすべてのグループに不利な状況で、私たちは気候変動に立ち向かえるのだろうか？体系的な人種差別についてはどうだろう？私たちに希望はあるのだろうか？

スノーデンの暴露から間もなく、私は市民的自由防衛センター（CLÐC）と提携しました。CLÐCは、「社会的不平等や環境破壊の根源となっている政治的・経済的構造の解体を目指す」社会運動に法的支援を提供する非営利団体です。CLÐCでは、社会運動の参加者を対象に、憲法修正第1条と第4条の権利（言論の自由と違法な捜索・押収を受けない権利）[1]をどのように守り、行使するかについて、「権利を知る」ためのトレーニングを行っています。これらの権利は、大量の監視によって損なわれます。憲法修正第4条[訳注1]の権利については明らかですが、憲法修正第1条の権利については、法学者がよく指摘するように、監視されていることを知れば市民は言論を制限するという萎縮効果があります。CLÐCの法律研修を補完するために、私は活動家向けのデジタルセキュリティ研修を定期的に開催するようになりました。この研修では、大量監視が行われている現代社会において、修正第1条および修正第4条の権利を守るためには、**暗号化が唯一の方法であるという前提に立っています。**この本は、こうした教育活動から生まれたものです。

「安全」なアプリをダウンロードするだけでは不十分

安全」なアプリをダウンロードするだけでは十分ではありません。まず、「安全」とは何を意味するのでしょうか。セキュリティは、複雑で主観的な多面的な概念です。リスクから完全に解放されることは通常ありえませんが、特にデジタル技術が関係する場合は、相対的に強力な保護が可能です。アプリの相対的な保護を評価したり、少なくとも説明したり（そしてグループの人々に利用してもらうよう説得したり）するためには、暗号技術や、

1 （訳注）修正第1条［信教・言論・出版・集会の自由、請願権］［1791年成立］ 連邦議会は、国教を定めまたは自由な宗教活動を禁止する法律、言論または出版の自由を制限する法律、 ならびに国民が平穏に集会する権利および苦痛の救済を求めて政府に請願する権利を制限する法律は、これを制定してはならない。」 修正第4条［不合理な捜索・押収・抑留の禁止］［1791年成立］「国民が、不合理な捜索および押収または抑留から身体、家屋、書類および所持品の安全を保障される権利は、これを侵してはならない。いかなる令状も、宣誓または宣誓に代る確約にもとづいて、相当な理由が示され、かつ、捜索する場所および抑留する人または押収する物品が個別に明示されていない限り、これを発給してはならない。」

特定のアプリやデジタルサービスを使用する際にどのような情報が危険にさらされるか（そしてその可能性）について、ある程度理解しておく必要があります。

私たちのトレーニングは、私が伝えたい情報の表面をなぞっているに過ぎません。ソーシャル・ムーブメントの参加者は忙しい人が多く、信頼できる人から簡単で実行可能なデジタル・セキュリティの推奨事項を教えてもらいたいと思っています。私がこの本で目指しているのは、オレゴン州立大学の関連コースである CS175.Communications Security and Social Movements です。この本（およびオレゴン州立大学の関連講座「CS175：Communications Security and Social Movements」）の目標は、こうした提言を行えるだけの知識を持つ人（少なくとも、その方法と場所を知っている人）を増やすことです。

この本の政治的範囲

憲法第 1 条と第 4 条に言及していることからもわかるように、本書は米国の政治の場に根ざしている。本書の多くは米国外でも通用するものですが、この知識を他の国で適用する場合には、追加のアドバイスを求めることをお勧めします。

この本の概要

本書は、以下の 3 つの理由から、包括的な内容を意図したものではありません。
1．好奇心旺盛な人なら誰でも読める本にしたい。暗号技術をさらに詳しく説明するには、大学レベルの数学が必要になります。また、デジタルセキュリティに関する合理的な提案をするために、特定の暗号プロトコル[2]を理解する必要はないと考えています。
2．大量監視の状況や、監視に対抗するためのアプリは常に変化しています。この本を仕上げるにあたり、国家の監視能力に関する最新のニュースを盛り込みたいという衝動に駆られています。
3．週末に読めるような短い本にしたいと思っています。

この本は、以下の 3 部構成になっています。

第 1 部 暗号技術の紹介

どのような情報が守られ、何が守られないのか、そしてその理由は何なのかという基本的なことを理解するのに十分な暗号技術の基本的な入門です。いくつかの興味深い概念（前方秘匿やブロックチェーンなど）は、こうした高度なトピックが私の想定する読者を圧倒するかもしれないと思ったので、省かれています。しかし、好奇心旺盛な読者は、パート 1 を読んだ後に、例えば、Wikipedia の記事で、前方秘匿やブロックチェーンなどのより高度なトピックを理解することができるはずです。

暗号プロトコルを説明の説明ではよく 3 人の人物が登場します。[3]アリスがボブにメッセージを送り、イヴがそれを盗聴しようとしているという場面です。この本と連携している講義では、公民権運動、特に黒人解放運動と、それらの運動に対する国家の弾圧に焦点

2（訳注）手順、手続

3（訳注）ブルース・シュナイアーの『暗号技術大全』(山形浩生訳、ソフトバンク・パブリッシング、2003、原書 1994 年)第二章に「登場人物」として配役表が示されている。慣例としてアリスを「すべてのプロトコルにおける一人目の参加者」とし、ボブを二人目とする。イブは盗聴あるいは傍受する者という役割りを担う。この他に、3 人目の参加者としてキャロル、4 人目がデイブ、邪悪な攻撃者をマロリーなど、役名が列記されている。こうした配役名を誰が最初に考案したのか訳者は確認していないが、シュナイアーのこの本は、出版年も早く、暗号学の古典でもあり、その影響は大きいのではないかと推測している。wikipedia「アリスとボブ」も参照。

を当てています。そのため、アリス、ボブ、イヴではなく、アサタがボビーと通信し、エドガーがそれを盗聴しているという例を用いています。

1．アサタ・シャカール Assata Shakur は（1970 年代前半に）黒人解放軍やブラックパンサー党のメンバーであり、「社会運動弾圧のメカニズム」の章で述べたように FBI の標的となり、現在もキューバで政治難民をしています。
2．ボビー・シール Bobby Seale は、公民権運動時代のブラックパンサー党の共同創設者であり、FBI による監視と嫌がらせを受けていました。
3．J．エドガー・フーバー J．Edgar Hoover は FBI を設立し、FBI の監視や抑圧の責任者とされています。本書では、必要に応じてエドガーを「The Man」と呼ぶことがあります（例えば、「The Man in the Middle」の章では、man-in-the-middle attack（中間者攻撃）が標準的な暗号技術の用語として使われています）。

この本の残りの部分は、今後数年のうちに大幅な更新が必要になると思われますが、第 1 部は時の試練に耐えることができるでしょう。

第 2 部：デジタルによる社会運動の弾圧（米国の場合）

このパートでは、次のようなかなり気が重くなる問題の概要が述べられています。

1．米国では歴史的に社会運動がどのように抑圧されてきたのか（そして監視がどのような役割を果たしているのか）を 「社会運動抑圧のメカニズム」の章で説明している。
2．「社会運動に対するデジタルの脅威」の章では、米国でどのような監視システムやその他のデジタルな脅威が使われているかを扱います。本パートでは、「国家」を、社会運動に対して広範な弾圧戦略と高度な技術的手段を展開する資源と動機を持つ確立された権力構造を代表する政府および非政府組織の集まりを指すものとして使用しています。

この部分は意図的に短くして、実際に実践できるようにするための最後の部に移ることができようにしています。第 2 部では、社会運動を弾圧するメカニズムがどのように利用されているのか、また、どのような種類の監視やその他のデジタル脅威が存在するのかを概観するために、いくつかの事例を取り上げます。特に「社会運動に対するデジタル脅威」の章は、常に新しい脅威や能力が開発・展開されているため、最新の情報を提供することができません。このパートをお読みになった方が、すぐに最後のパートに進んでくださることを願っています。

第 3 部：社会運動を守るために（アメリカ編）

第 3 部は、できるようになることを目的としています。脅威の分析（これは国や状況によって異なります）から始まり、情報を防衛するためのツールの分類に入ります。特定のツールではなく、ツールの分類と言ったのは、特定のツールは、そのツールやアプリをサポートするプロジェクトが登場したり失敗したりすることで、生まれたり消えたりする可能性がありますが、この本をこれに合わせて年に何度も更新するのは不可能だからです。このセクションは国によって異なります。特定のツールを利用できるかどうか、あるいはそれに関連するリスクは、あなたの政治的背景によって異なるからです。例えば、中国のように検閲が行われている国では、Tor（匿名性を提供するインターネットブラウザー）の使用が難しくなる場合があります。

次章で学ぶこと

暗号化とは？
社会運動の抑圧のメカニズム

外部リソース
市民的自由防衛センター. “About.”

パート 1：暗号技術の紹介

暗号化とは何か？
学ぶべきこと

Part1:暗号技術入門

暗号化とは何か？

学ぶべきこと
1．暗号化の基本要素：平文、暗号文、暗号（または暗号化プロトコル）、暗号鍵
2．古典的な暗号化手法の仕組み
3．暗号化が破られる可能性のある方法
4．破られない暗号
ここでは、「紙とペンを使った暗号」という基本的なものから始めて、コンピュータを使ったより複雑な暗号化方法に進んでいきます。
暗号化とは、メッセージにスクランブルをかけて、意図した相手だけが解読（読み取り）できるようにするプロセスです。元のメッセージ（平文）をスクランブルする方法は、暗号または暗号化プロトコルと呼ばれます。ほとんどの場合、暗号は秘密にすることを意図していません。スクランブルされた読めない暗号化されたメッセージは暗号文と呼ばれ、安全に共有することができます。ほとんどの暗号は、メッセージの暗号化と復号化（スクランブルとアンスクランブル）のために、暗号鍵と呼ばれる追加の情報を必要とします。

シンプルな暗号。シーザー暗号

まず，最も単純な暗号として，シーザー暗号を考えてみましょう。この暗号では，メッセージの各文字を，申し合わせておいた数だけアルファベットをシフトさせます。例えば，次のような平文を暗号化したいとします。
IF VOTING CHANGEÐ ANYTHING IT WOULÐ BE ILLEGAL

という平文を暗号化しようとした場合、メッセージの各文字をアルファベットの 3 つ分後にずらし、A を Ð、B を E、そして Ƶ をアルファベットの最初に折り返して C にします。この平文を暗号化すると、次のような暗号文になります。
li yrwlqj fkdqjhg dqbwklqj lw ƶrxog eh loohjdo
このメッセージを復号するには、受信者が逆の操作をします。メッセージの各文字をアルファベットの 3 つ前に戻して、Ƶ を W に、A をアルファベットの最後からさかのぼって X にします。受信者がメッセージを（素早く）解読するためには、暗号の鍵を知らなければならなりません。シーザー暗号では、各文字がアルファベットで何番目に移動したのか、その位置を表しています。この例では「3」となっています。シーザー暗号の鍵は、A からの変換結果に対応するアルファベットで表すこともできます。例えば、3 のシフトは Ð の鍵、23 のシフトは Ƶ の鍵、そしてゼロのシフト（同一性のシフト）は A の鍵となるでしょう。[4]

用語のおさらいをしておきましょう。この例では、暗号（または暗号化プロトコル）を適用するには、次の指示に従うだけでよい。「暗号化するには、平文メッセージの各文字をアルファベットの後方に n 文字ずつシフトシフトする。復号化するには、メッセージである暗号文の各文字を、アルファベットの前方に n 文字ずつシフトする」。鍵となるのはシフト量 n です。

もちろん，シーザー暗号は強力な暗号ではありませんし、自分の計画を秘密にしておくためにシーザー暗号を信頼すべきではありません。敵対者があなたの秘密のコード（暗号

4（訳注）「暗号を解く鍵は Ð だよ」と言えば、A を Ð に変換する、つまりアルファベット順で 3 つ移動させることを意味する。

文）を解読するために必要なことは、アルファベットを後方にシフトする可能性をすべて試すことです。鍵 A は暗号文と平文を等しくするものなので、これを除くと 25 個の鍵しかありません。このような攻撃は、可能な鍵をすべて試して暗号化されたメッセージを解読しようとする攻撃で、ブルートフォース攻撃[5]と呼ばれます。シーザー暗号の場合，可能な鍵が非常に少ないため、この攻撃が可能です。

少しだけ複雑な暗号。ヴィジュネル暗号

ヴィジュネル暗号は、複数のシーザー暗号を組み合わせたもので、それぞれに鍵があります。通常、鍵は単語として与えられ、その単語のアルファベットの位置によって、シーザー暗号のように A の文字をどのようにずらすかが決まります。これは、例を挙げて説明するのが一番わかりやすいでしょう。例えば、次の平文を暗号化したいとします。

RESPECT EXISTENCE OR EXPECT RESISTANCE
(存在を尊重せよ、さもなくば抵抗に遭う)

を ACT という鍵で暗号化したいとします。

このばあい

・平文の 1 文字目から始めて 2 つおきに現れる文字(R，P，T …)は、ACT 鍵の 1 文字目が A なので A を鍵とするシーザー暗号で暗号化します。このシーザー暗号は A を A に、R を R に、P を P に変換します。この鍵は 0 とも表されます。
・平文の 2 文字目から始めて 2 つおきに現れる文字(E，E，E …)は、ACT 鍵の 2 文字目が C なので C を鍵とするシーザー暗号で暗号化します。このシーザー暗号は A を C に、E を G に変換します。この鍵は 2 とも表されます。
・平文の 3 文字目から始めて 2 つおきに現れる文字(S，C，X …)は、ACT 鍵の 3 文字目が T なので T を鍵とするシーザー暗号で暗号化します。このシーザー暗号は A を T に、S を L に変換します。この鍵は 19 とも表されます。

この 3 つのシーザー暗号を適用すると、暗号文ができあがります。

rglpgvt gqiumepve qk ezieem rgliumapve

この暗号を破るには、敵が鍵の長さを知っているとします。敵は、その長さの 3 文字の単語（一般的には 3 文字の文字列）をすべて使って暗号文を復号しようとします。この例では、最大で 25 x 26 x 26 = 16,900 回の試行が必要になります。これは、人の手では簡単にできない量ですが、コンピュータでは容易にできます。もし敵があなたの鍵の長さを知らなければ、ブルートフォース法で暗号を解読するためには、さらに多くの可能な鍵（25 + 25 x 26 + 25 x 26 x 26 + … ）を試さなければなりません。鍵が長ければ長いほど、ブルートフォース法は難しくなり、敵対者は暗号を破るために苦労しなければならないことに注意してください。

コンテクスト：破れないワンタイムパッド

ヴィジュネル暗号は、ランダムに選択された文字列を鍵とし、少なくとも平文メッセージと同じ長さの鍵を使うことで、ワンタイムパッド onetime pad と呼ばれる暗号を作成することができます。歴史的には、鍵自体を紙に書いて通信相手に配布していました。暗号化にはヴィジュネル暗号を適用するのですが、暗号鍵としてワンタイムパッドから拾う文字はどれも一度だけ使い、平文の次の文字に対してはワンタイムパッドから次の文字を鍵として使います。復号化には、このワンタイム・パッドと鍵の開始位置が必要となります。鍵がなければ、この暗号を破ることはできません。つまり、時間と資源が無限にあっても、

5（訳注）ブルート・フォース brute force、「力づく」の意味、総当たり攻撃などとも呼ばれる。

鍵を推測して暗号文を解読することができないのです。これは、ある長さの暗号文が同じ長さの任意の平文に対応しうるためです。例えば、ランダムキーを知らない場合、ワンタイムパッドで暗号化された暗号文 SOU ÐUCYFUK RXL HQKPJ は、ALL ANIMALS ARE EQUAL という平文にも、FEW ANIMALS ARE HAPPY という平文にも、同じ確率で対応しうるのです。鍵がなければ、意図した（平文の）メッセージを知る手立てがまるでないのです。単語間のスペースを省略したり、単語間のスペースを暗号化したりすれば（27 文字のアルファベット ABCÐEFGHIJKLMNOPQRSTUVWXYZ_（_はスペース）を使用）、単語の文字数のパターンにあてはまる平文の組み合わせを推測することさえはるかに困難になります。

もちろん、ワンタイムパッドには、鍵（onetime pad 自体）をどのように通信相手と交換するかという実用上の問題があります。この鍵は、メッセージの長さと同じか、将来起こりうるすべてのメッセージの合計の長さと同じです。それにもかかわらず、歴史的には、グループでワンタイムパッドを直接共有して、安全でないチャンネルでメッセージを送信するという方法が使われてきました。1980 年代後半、南アフリカでアパルトヘイトと闘っていたアフリカ民族会議（ANC）は、海外の支持者と国内の工作員との間のメッセージを暗号化するためにワンタイムパッドを使用していました。ワンタイムパッド（鍵）は、アムステルダムからヨハネスブルグまでの路線を担当していた信頼できる航空スチュワードが物理的に輸送していました。ちなみに、ANC では暗号化と復号化をコンピュータ化しており、暗号化されたメッセージを電話回線で送信し、留守番電話に録音したり、留守番電話から受信したりすることで、"非同期通信(訳註)"を可能にしていました。

訳註：通信を行う機器間でデータや信号の送信と受信のタイミングを合わせる動作や仕組みを用いずに通信することを非同期通信という。(https://e-words.jp/w/%E9%9Ð%9E%E5%90%8C%E6%9C%9F.html)

次に学ぶべきこと

現代の暗号技術

図版の出典

Jenkin, Tim "Talking with Vula: The Story of the Secret Underground Communications Network of Operation Vula." (英語) Mayibuye: Journal of the African National Congress, October 1995.

現代の暗号技術

この章を読む前に、「暗号化とは」の章を読んでおくことをお勧めします。

この章で学ぶこと

1. 安全性と鍵の長さの関係
2. オープンソースソフトウェアとは何か、なぜそれがセキュリティにとって重要なのか

現代の暗号技術は、人の手で行うものではありません。コンピュータが代わりにやってくれるのですが、そのアルゴリズムの詳細については本書では触れません。しかし、現代のデジタル・セキュリティ・ツールをよりよく理解し、評価するのに役立つ一定の原則があります。

ブルートフォース・アタックを必要とするセキュリティ

現代の暗号プロトコルは、（暗号鍵を持たない）敵に、暗号解読のためにありとあらゆる可能な限りの鍵を試すだけの時間を（ほぼ）費やさせるように設計されています。可能な

限りの鍵を試すことはブルートフォース攻撃として知られていることを思い出してください。暗号プロトコルのパラメータ[6]は、ブルートフォース攻撃が実用にならないほどその計算に長時間を要するように設定されています。通常、最も重要なパラメータは、鍵の長さです。古典的なヴィジュネル暗号と同様に、鍵が長いということは、正しい鍵を推測するために、より多くの可能性のある鍵を探さなければならないということです。時代が進み、コンピュータの処理が高速化・高性能化すると、ブルートフォース攻撃が不可能であることを保証するために、より長い鍵が必要になることがあります。そのため、多くの暗号プロトコルでは、鍵のサイズを「鍵を表現するのに必要なビット数」で表しています。

コンピュータは、暗号鍵を含む情報を、0と1の2値で表現します。0から9までの数字が10進数の桁 digitsを表すように、0と1が2進数のビット bits(単位)を表します。3桁の10進数は何個あるでしょうか？10x10x10＝10^3＝1000、つまり0～999の数字です。同じように、4ビットの2進数は、2x2x2x2＝24＝16個あります。

例として、AES暗号プロトコル[7]を128ビット、256ビットの暗号鍵で使用する場合、AES-128、AES-256と呼ぶことがあります。AES-128では、2^{128}＝340282366920938463463374607431768211456個の鍵が考えられます。AES-256では、2^{256} ＝115792089237316195423570985008687907853269984665640564039457584007913129639936個の鍵が考えられます。AES-256のすべての可能な鍵、あるいは可能な鍵のごく一部でも試してみることは、米国のような国民国家の計算能力をもってしても、計算上不可能です。

隠匿では安全性を確保できない

19世紀初頭から、数学者は「暗号方式は、その方式が秘密でなくても安全でなければならない」という基準を持っていました。これは、「安全性を確保するために方式を秘密にしなければならないのであれば、これまでにその方式で暗号化された、あるいはこれから暗号化されるすべてのメッセージは、その方式が明らかになってしまう危険性がある」という原理に基づくものです。一方、鍵を秘密にしておくことだけが必要な方法であれば、その鍵が漏洩した場合に、その鍵で暗号化されたメッセージが明らかになってしまうリスクがあるだけです。

透明性がもたらすセキュリティ

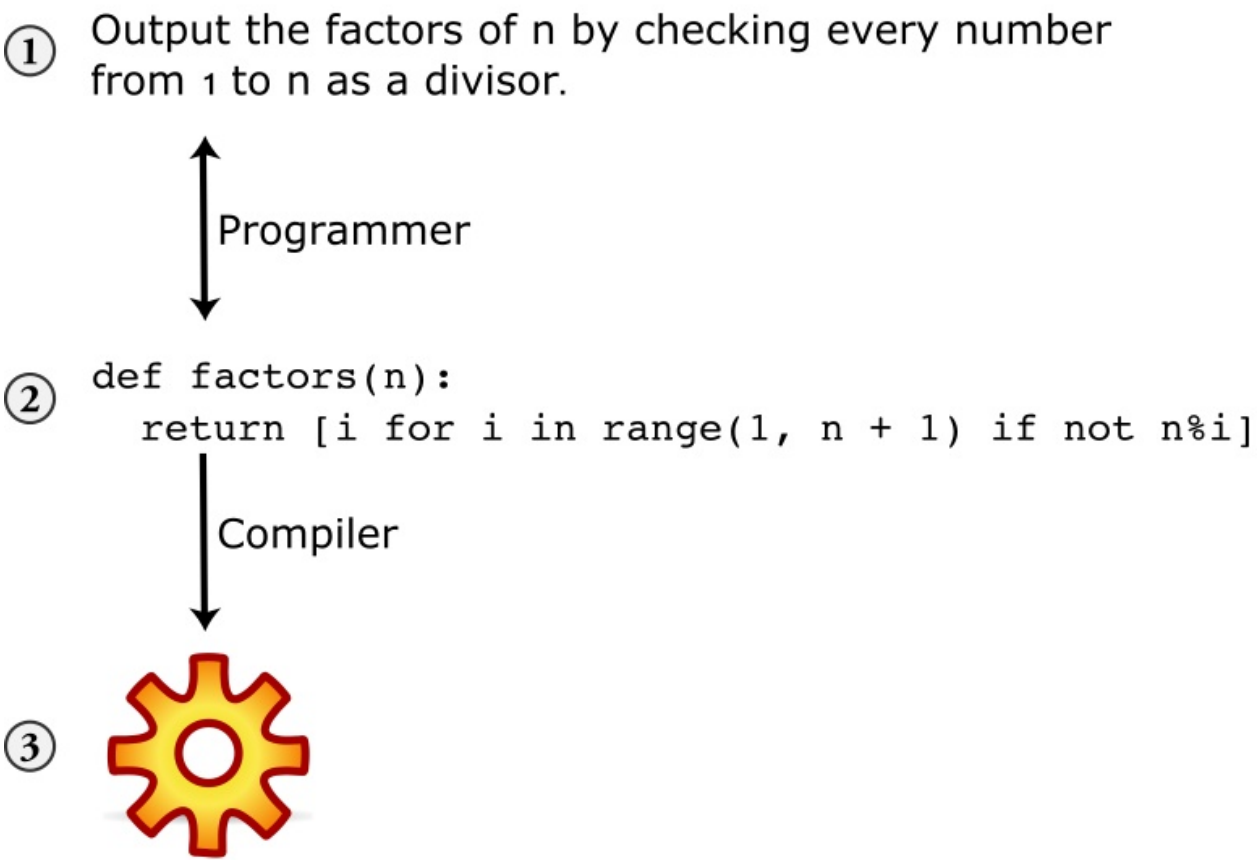
実際、暗号化方式の透明性が高ければ高いほど、その暗号化方式の安全性を信頼することができます。このことを理解するために、暗号化プログラム（あるいは他のコンピュータプログラム）がどのように作られるかを考えてみましょう。まず、暗号化を実行するためのアルゴリズムが作成されます。プログラマーは、このアルゴリズムをコンピュータのソースコードにします。コンピュータは、このソースコードをコンパイルして、あなたのコンピュータや携帯電話で動作するプログラムやアプリを作ります。[8]

---

6 （訳注）関数、機械、ソフトウェアなど何らかの仕組みに対して外部から与える値のことで、内部の構造や処理手順などが同じでも与えるパラメータによって出力や挙動を変化させることができる。https://e-words.jp/w/パラメータ.html

7 （訳注）AES(Advanced Encryption Standard) 2000年にアメリカ連邦政府標準の暗号方式として採用された、共通鍵（秘密鍵）暗号方式の一つ。「AES」は米国立標準技術研究所（NIST）の標準規格としての名称であり、暗号方式（暗号アルゴリズム）そのものを指す場合は「Rijndael」（ラインダール）と呼ばれることもある。特許などの許諾や対価の支払いの必要な技術を含まず、完全な仕様が公開されている。米政府関連の情報機器やシステムだけでなく様々な製品や技術規格などに採用され、共有鍵暗号の標準として全世界で広く普及している。身近な例では無線LAN（Wi-Fi）の通信の暗号化、インターネット上の通信を暗号化するSSL/TLS、圧縮ファイルの暗号化などで用いられている。https://e-words.jp/w/AES.html

8 （訳注）アルゴリズム：コンピュータにプログラムの形で与えて実行させることができるよう定式化された、処理手順の集合。
ソースコード：プログラミング言語などの人間が理解・記述しやすい言語やデータ形式を用いて書き記されたコンピュータプログラムのこと。



アルゴリズムからソースコード、コンパイルされたソースコードへ

優秀なプログラマーは、アルゴリズム（1）からソースコード（2）に変換し、さらに元に戻すことができるはずです。セキュリティの専門家であれば、アルゴリズムに基づいて暗号プロトコルの安全性を評価することができますが、同時にソースコードを評価して、その実装が忠実に行われているかどうか（意図的かどうかにかかわらず、間違いやバグがないかどうか）を確認する必要があります。しかし、ユーザーとしては、コンパイルされたプログラムにしかアクセスできません(3)。残念ながら、コンパイルされたコードしかない場合、誰もがソースコードを再現することはできません。そのため、ソースコードが入手できない限り、アプリのセキュリティに関する主張が正しいかどうかは誰にもわかりません。一方で、ハッカーがアプリのセキュリティを破ろうとするには、コンパイルされたプログラムだけあれば十分です。多くのソフトウェアプロジェクトがソースコードを公開しています。このようなソフトウェアはオープンソース・ソフトウェアと呼ばれ、Signal、Firefox、Linuxなど、セキュリティを含む多くの有名なプロジェクトが含まれています。もう一方はクローズドソースソフトウェアであり、Safari、Internet Explorer、Windows、Mac OSなど、プロプライエタリ[9]proprietaryなソフトウェアの販売を通じて製品を収益化することを目的としたプロジェクトで採用されています。クローズド・ソース・ソフトウェアのセキュリティを評価することは可能ですが（例えば、社内や依託での監査など）、それを継続的に維持することははるかに困難です。オープンソース・プロジェクトは、誰でも自由に調査することができるため、セキュリティ上の（あるいはその他の）問題を発見する機会があるのです。

コンパイル：プログラミング言語で書かれたコンピュータプログラム（ソースコード）を解析し、コンピュータが直接実行可能な形式のプログラム（オブジェクトコード）に変換すること。(いずれも下記の記述を引用。https://e-words.jp)

9 (訳注)「プロプライエタリ：商標［特許］で守られた、独占所有権のある」

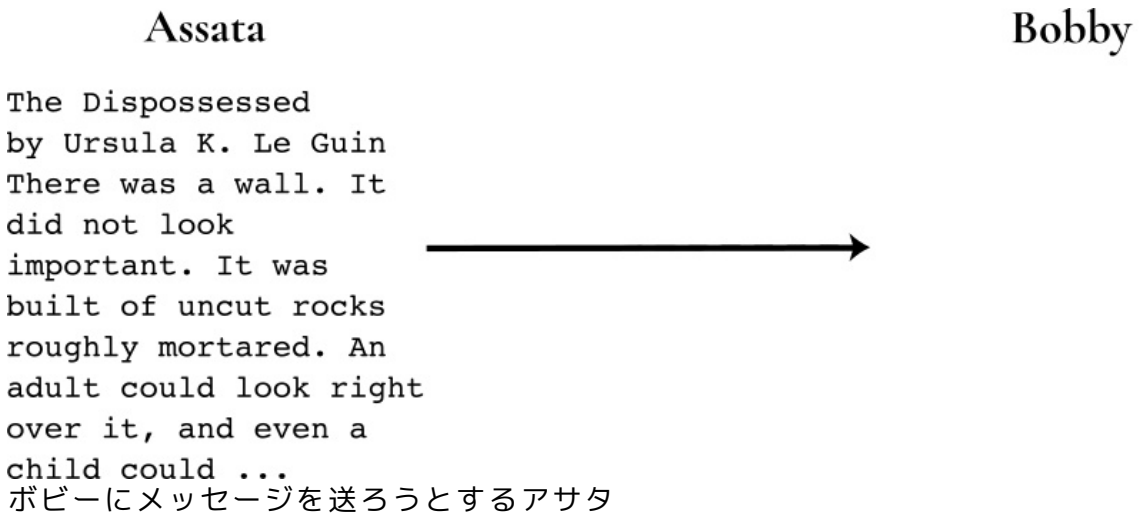
暗号化キーの保護によるセキュリティの確保

最近の暗号プロトコルでは、暗号化方式が一般的に公開されているため、セキュリティを確保するには、暗号化キーを保護する必要があります。実際にどのように保護するかは、暗号鍵がどこにあるかによって異なります。安全なインスタントメッセージングアプリである Signal の場合、暗号化キーは携帯電話内のファイルで、これが携帯電話の通信を保護しています。あなたのパスワードをクラウドと同期できるようなパスワード・マネージャーの場合、あなたのパスワードを全部保存しているファイルを暗号化する鍵は、パスワード・マネージャーにログインするときのパスワードから導出され保護されていています。

インフラへの不信感がセキュリティにつながる

エンド・ツー・エンドの暗号化とは、メッセージをスクランブルすることで、会話のエンドポイント(終点)でしか読めないようにすることです。しかし、ここで混乱が生じています。エンドポイントとは何でしょうか？エンドポイントとは、あなたとあなたの友人だけでしょうか？それとも、サーバーもエンドポイントなのでしょうか？これは、アプリケーションによって異なります。例えば、https (あなたがアクセスしたウェブページをホストするサーバーとあなたとの間の通信を保護する) は、あなたとサーバーだけがウェブページの内容を解読できるように暗号化されています。Signal はメッセージを暗号化して、あなたとあなたがメッセージを送っている友人だけが読めるようにします。どちらの場合も、情報を知る必要のある人や団体だけが情報を復号化することができます。これがエンド・ツー・エンド暗号化の本質です。

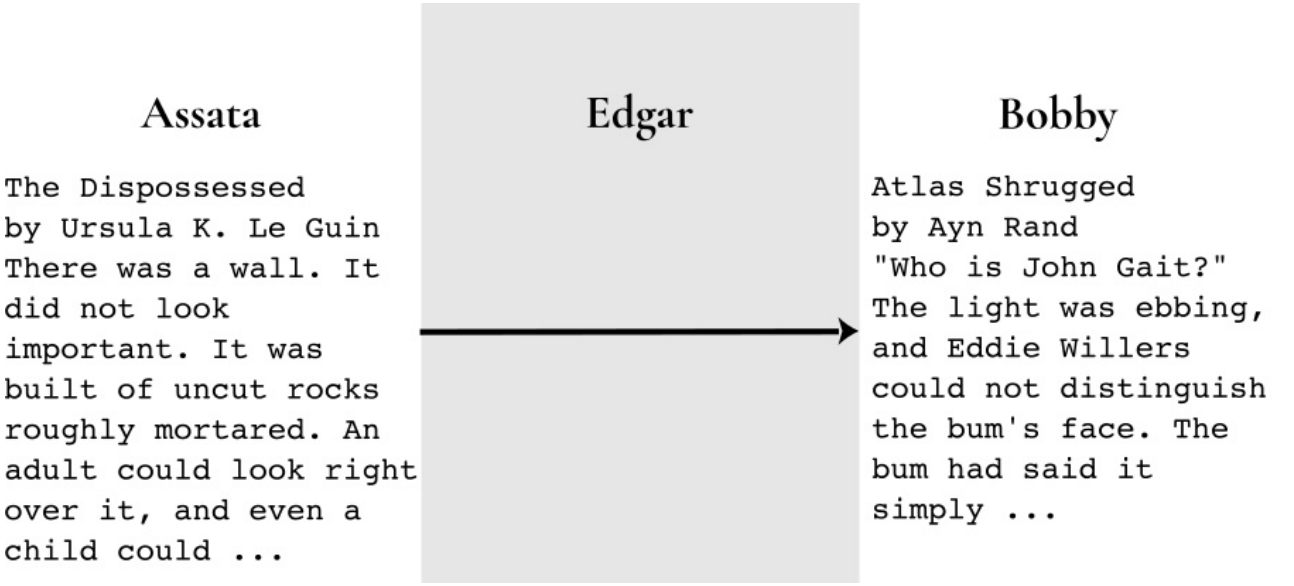
ここでは、プライベートメッセージングにおいてエンド・ツー・エンドの暗号化が重要な理由を説明します。これについては、「中間者」の章で詳しく説明しています。次の図では、アサタ (左) がインターネットを介してボビー (右) にメッセージ (アーシュラ・K・ル・グィンの『所有せざる人々』[10]) を届けようとしています。



ボビーにメッセージを送ろうとするアサタ

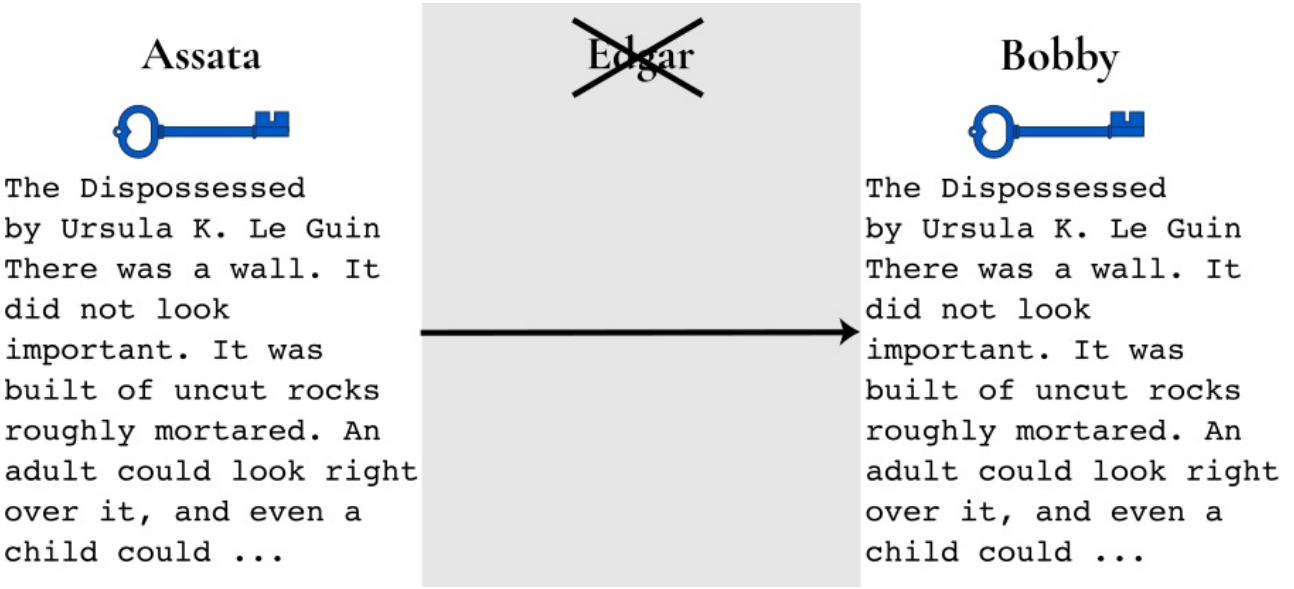
しかし、インフラには J.エドガー・フーバーの亡霊がつきまとっています。この中間者 (MITM, Man-In-The-Middle)は、二人の友人の間で送られる保護されていないメッセージを傍受し、読み、変更することができます。こんな感じです。

10 (訳注) ハヤカワ文庫 SF 例示の文章は、『所有せざる人々』の冒頭箇所。



間にいる者がメッセージを傍受して変更する(エドガーは、メッセージをそのまま読んで送ることもできる)[11]

さらに悪いことに、アプリが「暗号化」を使用しているといっても（誰が鍵を持っているかを明確にせずに）、メッセージのプライバシーが守られ本物であることは保証されません。例えば、2人の同志の間にあるサーバーが暗号化キーを管理している場合、そのサーバーにアクセスできる人は、2人の間のすべてのメッセージを読み、変更することができます。しかし、アサタとボビーがメッセージを（下図の青い鍵で）暗号化している場合、エドガーはメッセージを読むことができず、青い鍵で復号できるメッセージに置き換えることもできないでしょう。



暗号化によって、間にいる者によるメッセージの変更をできなくする

アプリケーションがエンド・ツー・エンドの暗号化を使用しているかどうかは、どうすれば分かるのでしょうか？暗号化キーを確認する方法があるということが最も良い方法といえます。Signal では安全番号 safety numbers を使ってこれを簡単に行うことができます。これについては、「暗号化された署名による真正性」の章で詳しく説明します。

11 （訳注）エドガーはル・グィンのかわりにアイン・ランドの『肩をすくめるアトラス』(アトランティスから日本語版)を送っている。アイン・ランドは米国の保守、右翼が愛読する作家として有名。他方、ル・グィンは、アナキストや左翼に人気のある SF 作家。

悪意ある第三者の影響を受けにくくするもう一つの方法は、ピア・ツー・ピア[12]のメッセージングで、メッセージや連絡先の管理の間に「サーバーが存在しない」ことだと言われています。あなたとあなたの友人の間には、膨大な量のインターネットインフラが存在していますが、ほとんどのユーザーやアプリケーションからは見えません。上述したように、このインフラこそが、国家が、検知されず疑われることなく大量監視を行うために利用するものなのです。

コンテクスト：エニグマ・マシン

最初の近代的な暗号化技術は、おそらく第二次世界大戦中に使用されたものです。現代のコンピュータに先駆けて、そのプロトコルは洗練された機械装置によって支えられていました。その中でも最も有名なのが、ナチスドイツが使用したエニグマ・マシンです。エニグマは電気機械式の装置で、特定の鍵を設定して平文を入力すると、暗号文が出力される仕組みになっていました。同じ鍵で、暗号文を入力すると、元の平文が出力されます。

エニグマ・マシン（写真提供：Greg Goebel

ここでの鍵とは、ローターの順番と初期位置（上の写真）のことです。標準的な操作では、毎日新しい鍵を使わなければなりませんでした。エニグマ・マシンのオペレーターに配布されたハンドブックには、日々の鍵が記載されており、これは実質的にワンタイムパッドです。ちなみに、このハンドブックは水溶性のインクで印刷されているので、敵の手に渡る恐れがあるときはすぐに破棄することができました。

エニグマで暗号化されたメッセージを解読するには、多くの努力が必要でした。第二次世界大戦中にいくつかの機械が接収されましたが、機械を手に入れてもメッセージを解読することはほとんど不可能でした（方法が公開されている現代の暗号と同様です）。コンピュータ科学の創始者の一人であるアラン・チューリングは、第二次世界大戦中、英国の暗号解読者の中心地であるブレッチリー・パークで働いていました。チューリングが設計したボンベ bombe は、エニグマのメッセージを解読するために特別に設計されたコンピュータの一種です。しかし、ボンベだけでは不十分でした。(実際、鍵なしでエニグマのメッセージを解読することは、現代の計算能力をもってしても非常に困難であり、戦時中に傍受されたエニグマ暗号でまだ解読されていない有名なメッセージが少なくとも 1 件はあります。）。しかし、ボンベと、早朝のメッセージのほとんどが天気予報や「Keine besonderen Ereignisse」（「何も報告することはない」）というフレーズを含んでいた

12 (訳注)ピア・ツー・ピア(P2P)ネットワーク上で機器間が接続・通信する方式の一つで、機能に違いのない端末同士が対等な関係で直に接続し、互いの持つデータや機能を利用しあう方式。また、そのような方式を用いるシステムやソフトウェアなどのこと。(https://e-words.jp/w/P2P.html)

という事実とが相まって、連合国側はエニグマの暗号化されたメッセージを定期的に解読することができました。

戦時中のチューリングの功績は、戦争を 2 年以上も短縮したと言われています。しかし、ブレッチリー・パークでの仕事は機密扱いだったため、彼の仕事は生涯知られることはなく、実際、彼は戦争に貢献していないと批判されていました。さらに悲劇的なことに、同性愛者である彼は、政府から迫害され、1952 年には同性愛の罪に問われました。有罪となった彼は、化学的な去勢手術か投獄かの選択を迫られました。懲役刑を選択した彼は、あと 2 年しか生きられず、青酸カリの毒で自らの命を絶ったと言われています。

次に学ぶこと

暗号化のための鍵の交換

図版の出典

Caraco, Jean-Claude, Rémi Géraud-Stewart, and Ðavid Naccache. “Kerckhoffs’ Legacy.” 2020.
メディア掲載情報

source-code © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license
mitm-basic-1 © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license
mitm-basic-2 © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license
mitm-basic-3 © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license
Four-rotor-enigma © Greg Goebel is licensed under a Public Ðomain license

暗号化のための鍵の交換

本章を読む前に、「現代の暗号」の章を読むことをお勧めします。

学ぶこと

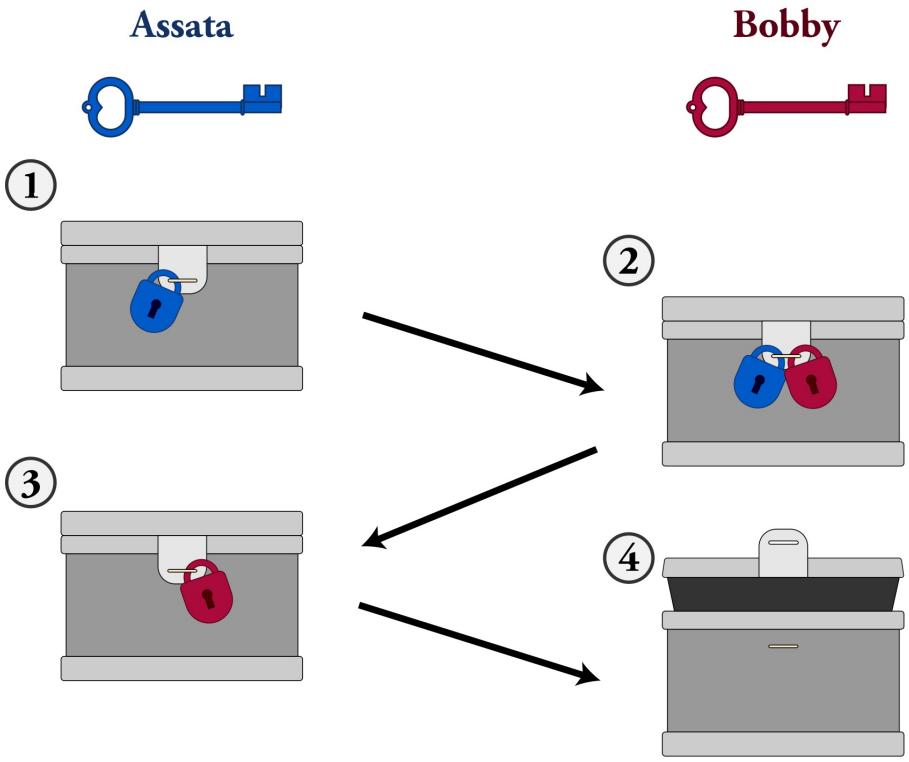
1. 暗号化キーを事前に共有せずにメッセージを暗号化する方法
2. 現在オンラインで行われている主な鍵の交換方法

インターネットを介した通信の盗聴は、直接接続している Wi-Fi ホットスポット、インターネットサービスプロバイダー、閲覧した Web ページをホストしているサーバー、各国のゲートウェイ、そしてその間にある膨大な数のルーターやスイッチなど、多くのポイントで行われています。暗号化されていなければ、これらの通信はすべて、ストーカーやハッカー、政府機関などの盗聴者に読まれてしまいます。しかし、通信を暗号化するためには、通信相手との間で鍵を取り交わす必要があります。Web サイトを閲覧する場合、その Web サイトを運営するサーバーと安全に鍵を交換するにはどうすればよいのでしょうか。インターネットのような安全ではない経路でしか通信できない 2 つの当事者（2 人、1 人と 1 台、2 台のサーバーなど）が、会うことなく効率的に鍵の合意をする方法が必要です。

物理的な例。鍵を交換せずにメッセージを交換する場合

まず、物理的な例を以下に示します。アサタがボビーに荷物を送りたいとします。彼女はその荷物を、複数のロックをかけた大きな留め具のついた丈夫な箱に入れます(1)。彼女

は箱にロックをかけましたが、ボビーはこれを開ける鍵を持っていません。アサタはボビーに箱を郵送しますが、ボビーは箱を開けることができません（箱が輸送されている間は誰も開けられません）。ボビーは箱を自分でロックします(2)が、これを開ける鍵をアサタは持っていません。箱を受け取ったアサタは、自分の鍵を外してボビーに箱を送り返します(3)。これでボビーは箱を開けることができるようになります。箱を開けようとする他の者は、アサタの鍵、ボビーの鍵、またはその両方を破らなければなりません。



鍵を共有せずに安全なメッセージを交換する

このように、鍵を交換しなくても、何かを安全に送信することは可能です。しかし、暗号化キーを交換するために、物理的にロックされた箱を郵送するわけにはいきません。そこで必要になるのが、デジタル通信に使える数学的なバージョンです。

数学的な例。鍵を交換せずにメッセージを交換する方法

では、物理的な箱や鍵を使わずに、どのようにして暗号化を行うかを考えてみましょう。例えば、(いつものように)任意のテキストを暗号化することができ、(ここでもいつものように)複数の暗号化レイヤー[13]を適用することができ、レイヤーの暗号化と復号化をどのような順序で行っても同じ結果が得られるような暗号化プロトコルがあるとします。この最後の性質を満たす数学的操作は、「可換 commutative」と呼ばれます。（「暗号化とは何か？」の章で説明した暗号化プロトコルはすべて可換です）それでは、ヴィジュネル暗号を例にして説明します。

13（訳注）層、階層、層にする、層をなす、などの意味を持つ英単語。何かの構造や設計などが階層状になっているとき、それを構成する一つ一つの階層のことをレイヤーという。

Assata は次のようなメッセージを暗号化します。

AT ONE TIME IN THE WORLÐ THERE WERE WOOÐS THAT NO ONE OWNEÐ
(世界のある時代には、誰も所有していない森があった。)

というメッセージを、ヴィジュネル暗号と鍵 ALÐO で暗号化し、暗号文を得ます。

ae rbe elae tq hhp zcrwg hhpus wpus wzrrs ekot yr cnp rknpg

と入力し、その結果を Bobby に送ります。Bobby は鍵を持っていません! しかし、Bobby はこの暗号文を ヴィジュネル暗号と LEOPOLÐ の鍵で暗号化し、二重に暗号化されたテキスト

li fqs poli hf vss kgflu skayg ldfv hdfgg pnzx mg qys cobeu

を得ます。

その結果を Assata に送り返します。Assata は Bobby からのメッセージを自分の鍵 (ALÐO) で“復号“し、(暗号化されたままのメッセージ)

lx ccs elxi wc hsh hsfar ekpvs lsch hscsg eklx bd cyh zabtr

を取得し、その結果を Bobby に送ります。

最後に、Bobby は自分の鍵 (LEOPOLÐ) でこれを解読し、Assata が最初に Bobby に送りたかったメッセージを得ます。

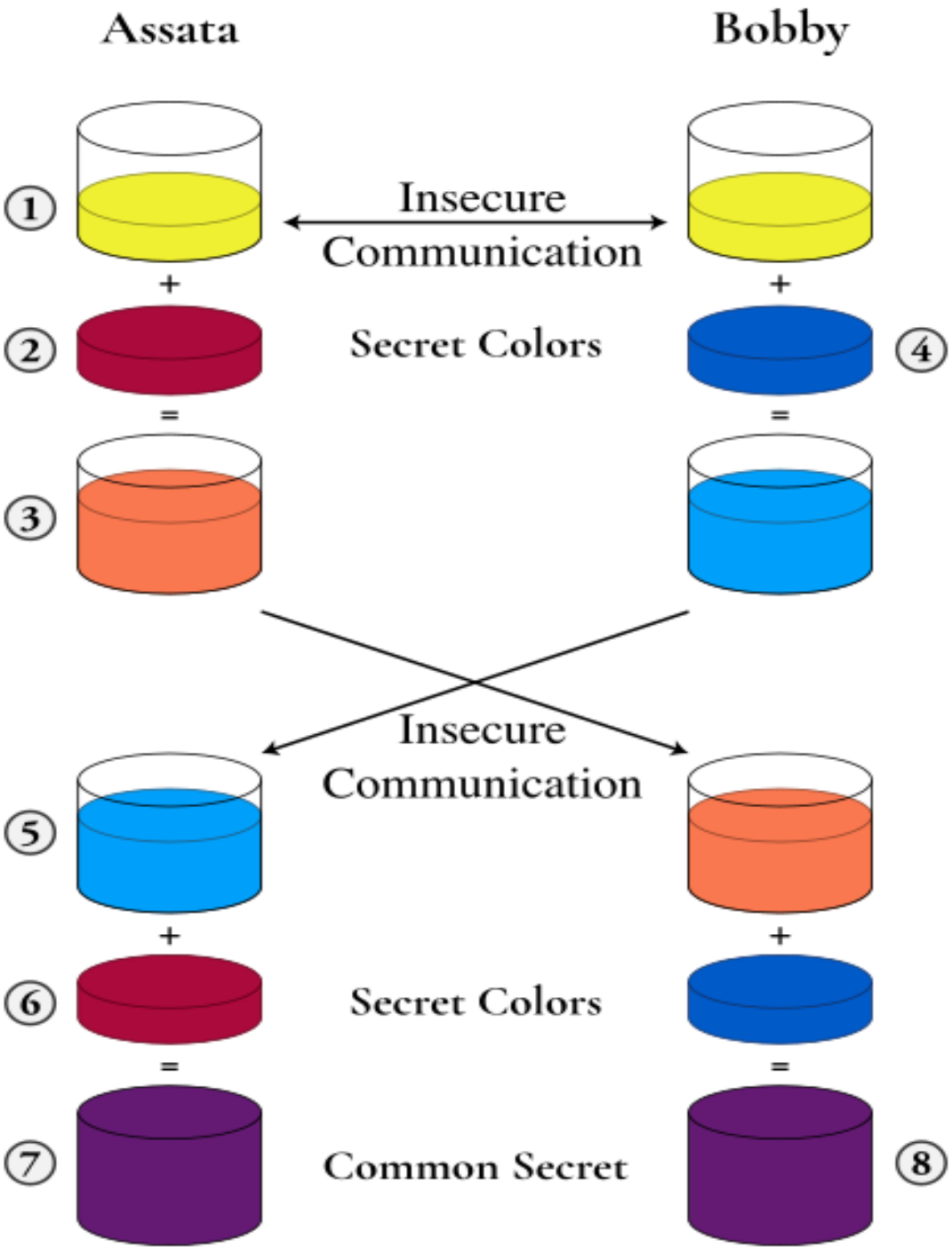
AT ONE TIME IN THE WORLÐ THERE WERE WOOÐS THAT NO ONE OWNEÐ
(世界のある時代には、誰も所有していない森があった。)

この例では、アサタは自分の鍵 (ALÐO) を誰とも共有しておらず、ボビーも自分の鍵 (LEOPOLÐ) を誰とも共有していないことに注意してください。ヴィジュネル暗号は可換であるため、メッセージがアサタの鍵で暗号化され、次にボビーの鍵で暗号化され、次にアサタの鍵で復号化され、最後にボビーの鍵で復号化されても問題はありません。重要なのは、メッセージがそれぞれの鍵で一度ずつ暗号化され、復号されたということです。盗聴者は、3 つある中間暗号文のいくつかを見ることしかできません。

物理的な例。安全でないチャンネルでの秘密の合意

現代の暗号システムでは、メッセージ全体を何重かに暗号化してやり取りするのではなく、上記の例とほぼ同じように、目的の通信に使用する鍵を決定するために、最初のやり取りを行います。アサタは、「AT ONE TIME IN THE WORLÐ…」というメッセージを送信するのではなく、より長い通信に使用するための暗号化キーを送ったと考えてください。これから、現代のほとんどすべての通信で使われている Ðiffie–Hellman 鍵交換と呼ばれる鍵交換の数学的基礎を説明します。

まず、数学の代わりに絵を使って、どのように行われるかを見てみましょう (下図)。ここでは、2 色の絵の具を混合し、この二つの絵の具の混合を解除する[もとの二つの色に戻す]ことはできないと仮定します。具体的には、2 色のうちの 1 色が何であるかを知っていても、それに何の色を混ぜて、結果的に混ざった色になったのかを知ることはできないと仮定します。



Crafting a shared secret, in paints

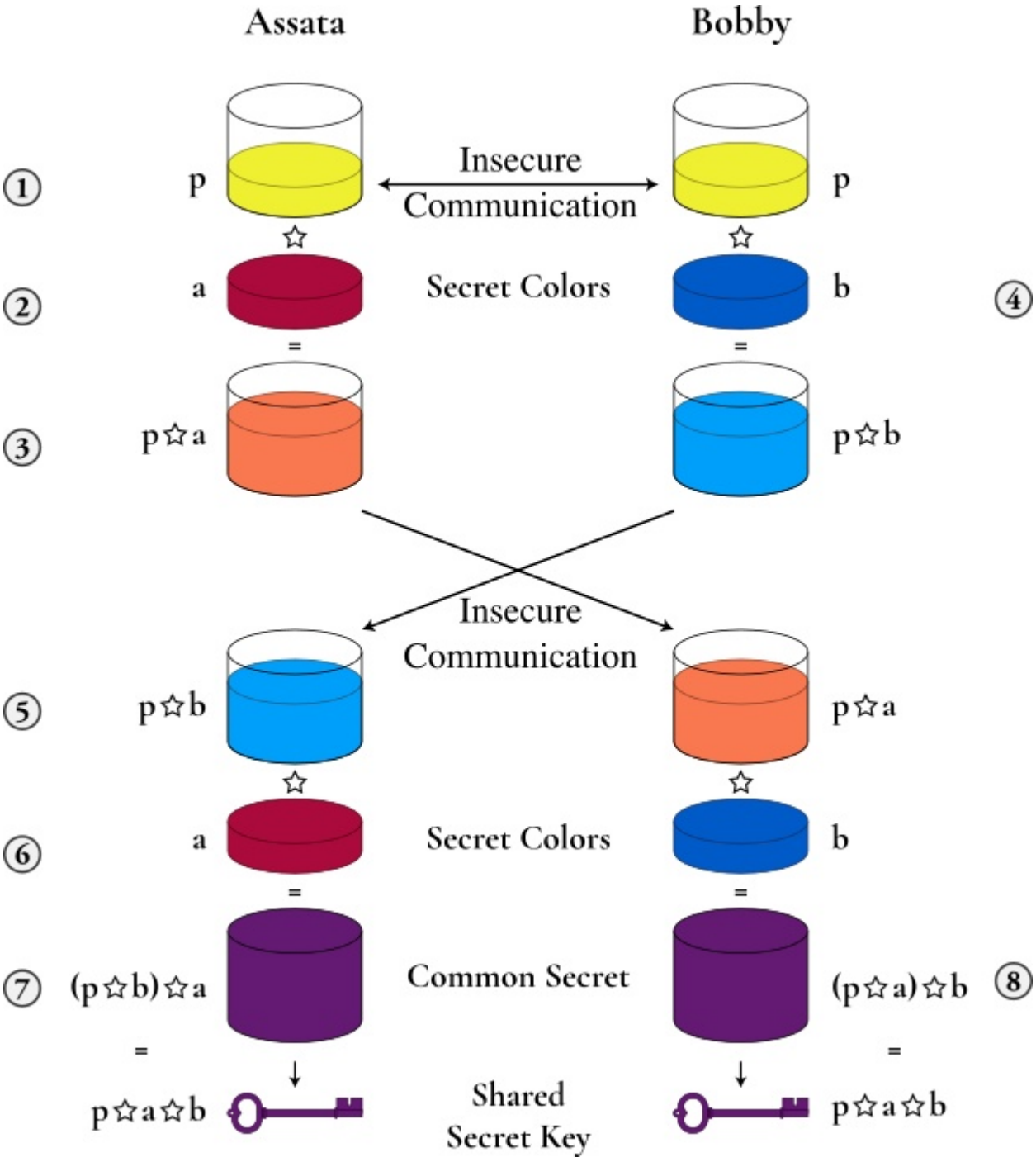
アサタとボビーは、まず絵の具の色（この例では黄色）と量（例えば 10mL）に合意します（1）。これは安全ではない通信経路で行うことができ、盗聴者には色と量もわかってしまうことを想定します。次に、アサタは色(ここでは錆びたオレンジ)を選び、それを秘密にします(2)。彼女は黄色 10mL と錆びたオレンジ 10mL を混ぜて、珊瑚色のような色にします(3)。彼女はこれを、盗聴者に見られてしまうことを承知の上で、安全ではないチャンネルを使って Bobby に送信します。Bobby も同じように、自分の秘密の色を使います(4)。

次に、アサタが Bobby から受け取った絵の具のサンプルを見てみましょう(5)。アサタは自分の秘密の色(6)を 10mL 混ぜて、濃い紫(7)にします。ボビーも同じことをします。黄色、彼女の秘密の色、そして Bobby の秘密の色をそれぞれ 10mL ずつ混ぜると、Assata の不快な茶色っぽい暗い紫色が得られます。ボビーの絵の具の混合物は、黄色と彼の秘密の色とアサタの秘密の色を 10mL ずつ混ぜ合わせて得られます。つまり、Bobby も同じように不快な茶色っぽい暗い紫(8)になってしまうのです！ 盗聴者はこの暗い紫色を作ることができるのでしょうか？盗聴者は、黄色(1)、黄色とアサタの秘密の色の組み合わせ(3)、黄色とボビーの秘密の色の組み合わせ(5)を盗み見しています。しかし、不快な茶色を作るためには、盗聴者はアサタかボビーの秘密の色を得るために混合を解除する必要がありますが、それはできません。

ディフィー・ヘルマン鍵交換(Diffie-Hellman Key Exchange)

このプロセスを数学的に再検討してみましょう。ここでは、元に戻すことは不可能か困難で、しかも可換式の数学的操作を用います。逆転が困難な数学的演算や関数は一方向性関数と呼ばれます。この数学的操作を記号☆で表してみましょう。つまり、ある数 a、b、c に対して、a ☆ b = c となるとします。「可換」とは、a ☆ b = b ☆ a ということです。実際には、ブルートフォース攻撃 (またはブルートフォースに近い攻撃) によってのみ、a に対してあらゆる可能性を試すことで、a が何であるかを知ることができるはずです。☆は乗算記号のようなものと考えてもよいでしょう。(なお普通の乗算は可換ですが一方通行ではありません。数学に興味のある方へ： 実際の Diffie-Hellman では、☆をべき剰余で実装できます。)

下の図は、アサタとボビーがある数字 p に合意し、それを公開(1)します。アサタは秘密の数 a を選び(2)、p ☆ a を計算し(3)、その結果をボビーに送ります。ボビーは秘密の数字 b を選び(4)、p ☆ b を計算して、その結果をアサタに送ります(5)。アサタはボビーからのメッセージ(5)と自分の秘密番号(6)を使って、(p ☆ b) ☆ a (7)を計算します。ボビーは, アサタからのメッセージ(3)と自分の秘密の番号(4)を使って, (p ☆ a) ☆ b (8)を計算します. ☆は可換なので、(p ☆ b) ☆ a = (p ☆ a) ☆ b となり、アサタとボビーがそれぞれ計算しても、同じ結果になるのです。盗聴者は p ☆ a, p ☆ b, それに p しか知らず、☆は一方通行なので、盗聴者はアサタとボビーの共有共通番号を計算する効率的な手段を持っていません。それはアサタとボビーの秘密です。アサタとボビーは、この共有する数を暗号鍵として使用することができます。



秘密鍵の合意

ディフィー・ヘルマン鍵交換の利用

ディフィー・ヘルマン鍵交換は、暗号鍵を合意するための手段としてあちこちで使用されています。この鍵交換は、皆さんが遭遇するほとんどの暗号化通信の基礎として使用されています。特に、https で Web サイトに接続する際の鍵交換の基本となっています。あなたがウェブサイトにアクセスするとき、URL は `http://` または `https://` で始まります。前者の場合、ウェブサイトのサーバーとの通信は一切暗号化されません。後者の場合、通信は暗号化され、その通信を暗号化するための鍵はディフィー・ヘルマン鍵交換で生成されます。

コンテクスト： 良いことが悪いことに

アサタとボビーが最初に行うことは、鍵交換の基礎となる数字 p に合意することです。この数字は公開されていますが、私たちは数学の演算☆が一方通行であることを前提にしていたので、p が公開されていても問題ありませんでした。しかし、多くの計算資源を持っている人（裕福な国民国家など）は、2 つの段階を経て（現実世界で☆に使われているべき剰余などの関数の）演算☆を反転させることができます。第 1 段階は、非常に長い時間をかけて、特定の p の値に対して行わなければなりません。第 2 段階は、第 1 段階が完了していると仮定して、同じ p の値に対して非常に早く（リアルタイムで）行うことができます。つまり、同じ値 p を使用するのではなく、異なる値 p を使用し、頻繁に変更するべきなのです。

しかし、2015 年に研究者が示したところによると、上位 100 万の https ドメインのうち 18% が同じ値 p を使用しているとのことです。ディフィー・ヘルマン鍵交換に依存している通信プロトコルには、他にも SSH（secure shell）と VPN（virtual private network）があります。同じ研究者は、SSH サーバーの 26% と VPN サーバーの 66% がディフィー・ヘルマン鍵交換に同じ値の p を使用していることを示しました。これは、強力な敵が暗号を解読するのにほとんど苦労しないことを意味します。

ディフィー・ヘルマンプロトコルは強力で信頼性の高いものですが、プロトコルを実装する側は、実際に安全であることを確認するために慎重に行う必要があることが浮き彫りになりました。

次に学ぶべきこと

中間者
公開鍵暗号方式

外部リソース

Adrian, Đavid, Karthikeyan Bhargavan, Žakir Đurumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, et al. *“Imperfect Forward Secrecy: How Điffie-Hellman Fails in Practice.”* In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 5–17. デンバー。ACM, 2015.

図版の出典

lockbox © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license
diffie-hellman-concept © Lorddota adapted by OSU OERU is licensed under a CC BY-SA (Attribution ShareAlike) license
diffie-hellman © Lorddota adapted by OSU OERU is licensed under a CC BY-SA (Attribution ShareAlike) license

暗号化ハッシュ

(訳注：前項で「次に学ぶべきこと」として記載されている「中間者」はこの次に説明されています)

本章を読む前に、「現代の暗号」の章を読むことをお勧めします。

この章で学ぶこと

1．ハッシュ関数とは何か
2．暗号ハッシュ関数とは何か、通常のハッシュ関数との違いは何か
3．暗号化ハッシュ関数の使用例

ハッシュ関数とは、任意の大きさのデータ（名前、文書、コンピュータプログラムなど）を、固定の大きさのデータ（3桁の数字、16ビットの数字など）に変換する（コンピュータの）関数のことです。ハッシュ関数の出力は、（入力メッセージの）ダイジェスト、フィンガープリント、ハッシュ値、またはハッシュと呼ばれます。

暗号化ハッシュ関数は、以下のような特性を持ち、暗号化アプリケーションにとって有用なものです。

1．同じメッセージは常に同じ出力ハッシュになる。
2．入力メッセージから出力ハッシュ値を生成することは、ブルート・フォース（可能な入力メッセージをすべて試す）以外では不可能である。
3．同じ出力ハッシュ値になる2つの異なる入力メッセージを見つけることは不可能である。
4．入力メッセージへの小さな変更は、新しいハッシュ値が元のハッシュ値と無相関に見えるほど、出力ハッシュ値が大きく変化する。

これらの特性のうち、最初の2つはほとんどの暗号化プロトコルと同じ性質のものです。同じメッセージを2回別々に暗号化した場合、同じ暗号鍵を使用していると仮定すれば、同じ結果が得られるはずです。暗号文だけしかなければ、（復号鍵なしで）平文を生成することは不可能なはずです。しかし、暗号化は、復号鍵を使って、暗号文から平文へと遡ることができます。ハッシュ関数は本質的に一方通行であり、逆のことができるための鍵はありません。暗号ハッシュ関数の出力は、（暗号文のように）入力メッセージのすべての情報を暗号化しているわけではありませんが、入力を識別するのに十分な情報を暗号化しており（性質1と3に依存）、これを偽造することは極めて困難です（性質2）。

暗号ハッシュ関数の応用例は、「中間者」「パスワードについて」「公開鍵暗号方式」の章で紹介しますが、ここでは簡単な使い方として、コミットメント・スキーム commitment scheme を見てみましょう。

自分の頭の良さを証明する暗号化ハッシュ関数の使い方

アサタとボビーの二人が難しい数学の問題を解こうとしています。アサタは先に答え(S)を手に入れ、、ボビーに答えを漏らさずに、ボビーが解く前に自分が答えを持っていることを証明したいと考えています。そこで、アサタは解答Sの暗号化されたハッシュをhash(S)とし、ボビーにhash(S)を渡します。ハッシュは暗号化されているので、ボビーはhash(S)からSを知ることはできません（性質2）。ボビーが最終的に問題を解き、自分でSを見つけたとき、彼はhash(S)を計算し、その結果がアサタが彼に与えたものと同じであることを確認することができます。特性1と3により、ボビーはアサタのハッシュ関数への入力と自分のハッシュ関数への入力が同じに違いないことがわかり、アサタが先に問題を解決したことが証明されます。(特性4はここでは使われていませんが、この特性がないと、アサタが正解に近いが正解ではない解を得た場合、2つの出力は非常に似ていて、ざっと比較しただけでは違うことがわからない可能性があります)

ハッシュ関数はどのようなものか？

現在、様々な暗号ハッシュ関数が使われていますが、それらを詳細に説明することは、本書の範囲を超えています。しかし、どのようなものかを知るために、暗号ハッシュ関数が持つ特性のすべてではないですが、いくつかの特性を満たす例を挙げてみよう。

ここでの例のハッシュ関数は、**chunked XOR** と呼ばれるものです。[14]排他的、あるいは **XOR** とは、一対の入力が与えられたときに、入力が異なる場合は真（または 1）を出力し、そうでない場合は偽を出力する関数です。つまり、例えば、**リンゴ XOR バナナ＝1、リンゴ XOR リンゴ＝0、0 XOR 1＝1、1 XOR 1＝0** となります。2 進数（0 と 1）の XOR の連鎖を取ると、意味のある答えが得られます。すなわち、**1 xor 1 xor 0 = 0, 1 xor 1 xor 0 xor 1 = 1** です。**XOR** は、2 進数の列に対して、連鎖の中に奇数個の 1 があれば **1** を、そうでなければ 0 を返します。

chunked XOR は、2 進数の入力で動作します。(入力が 2 進数でない場合は、コンピュータの場合と同じように、まず 2 進数で表現します)。入力をハッシュ関数の出力サイズと同じ大きさのチャンク（例えば 8 ビットのグループ）にグループ分けします。その塊を縦に並べて、各列の内容を **XOR** すると、下図のようになります。[15]

```
        input: 00111011 11101101 00101000 00101011 01011000 11001110

      chunked: 00111011
               11101101
               00101000
               00101011
               01011000
               11001110

XOR'd columns: 01010011 (output)
```

これは、入力の長さに関係なく、出力が常に同じ長さ（この例では 8）になるという点で、ハッシュ関数です。**chunked XOR** は、暗号ハッシュ関数の最初の特性を満たしていることがお分かりいただけると思います。しかし、残りの特性についてはうまくいっていません。例えば、入力メッセージ(必ずしもあなたの望むような入力メッセージだとは限りませんが)を所与の出力ハッシュで生成することは簡単です。例えばハッシュの結果に 11111111 11111111 を連結すると、そのハッシュとなる入力メッセージが作れるのです。
同じ理由から、同じ出力ハッシュとなるメッセージをいくつでも作ることができます。最後に、入力メッセージの 1 ビットだけ変更してみると、出力ハッシュは 1 ビットしか変化しません。

コンテクスト： 暗号化ハッシュは憲法修正第 4 条の権利を侵害する

2008 年、米国の地方判事は、米国政府が個人のデータを暗号ハッシュ化したい場合は、まず令状が必要であるという判決を下しました。この事件では、ペンシルバニア州司法長官(the Pennsylvania Office of the Attorney General)事務所の特別捜査官が、容疑者のコンピュータのハードドライブをコピーしました。特別捜査官は、コピーの暗号ハッシュを計算しました（特性 1 と 3 を利用して、改ざんしていないことを証明するために、後からオリジナルと比較できるようにしたのです）。次に、フォレンジックツールを使って、コピーしたハードディスク上の個々のファイル（削除されたがまだ上書きされていないファイルを含む）の暗号ハッシュを計算し、これらのハッシュを、禁制品ファイルのデータベースにあるファイルのハッシュと比較しました。捜査官は、ハードドライブ上のファイルのハッシュと禁制品ファイルのハッシュの間に 3 つのマッチを発見しました。プロパティ 1 と 3 により、ハードドライブには少なくとも 3 つの違法ファイルが含まれてい

14 (訳注)XOR:exclusive OR, 排他的論理和、エックスオアト読む。Chunk:かたまりの意。
15 (訳注 XOR'd columns の値は、縦に計算した結果を表示している。01000011 かもしれない。

ることになります。この事件を担当した裁判官は、この行為（ファイルをハッシュ化して既知のハッシュと比較すること）がハードドライブの捜索にあたると判断し、違法な捜索や押収からの保護に関する被告人の憲法修正第4条の権利を侵害したとしました。その結果、この証拠は裁判で使用することができませんでした。

私たちは、児童ポルノの所持に関わるこの事件の詳細を開示すべきだと考えています。私たちは、児童ポルノの所持（または作成や配布）の権利を擁護することはありませんが、権力（この場合は、コンピュータ上の特定のファイルの存在を決定する権力）が、例えば、友人があなたと共有していた音楽、原油流出の画像、#blacklivesmatterデモの画像、Earth First![16] ジャーナル記事とか、利用されたくないやり方でで利用する場合のことを想定することは重要です。

次に学ぶべきこと

パスワードについて
中間者
暗号化された署名による真正性

外部リソース

アメリカ合衆国 v. ロバート・エルズワース・クリスト（III）、被告。刑事訴訟番号1:07-cr-211。627 F.Supp.2d 575 (2008).

中間者[17]

本章をお読みになる前に、「暗号化のための鍵の交換」および「暗号化ハッシュ」の章をお読みになることを勧めします。

学ぶべきこと

1．なりすまし攻撃とは何か

2．中間者攻撃とは何か

3．受動的中間者攻撃と能動的中間者攻撃の違い

4．フィンガープリンティングを使って、鍵交換時に受けた中間者攻撃を発見する方法

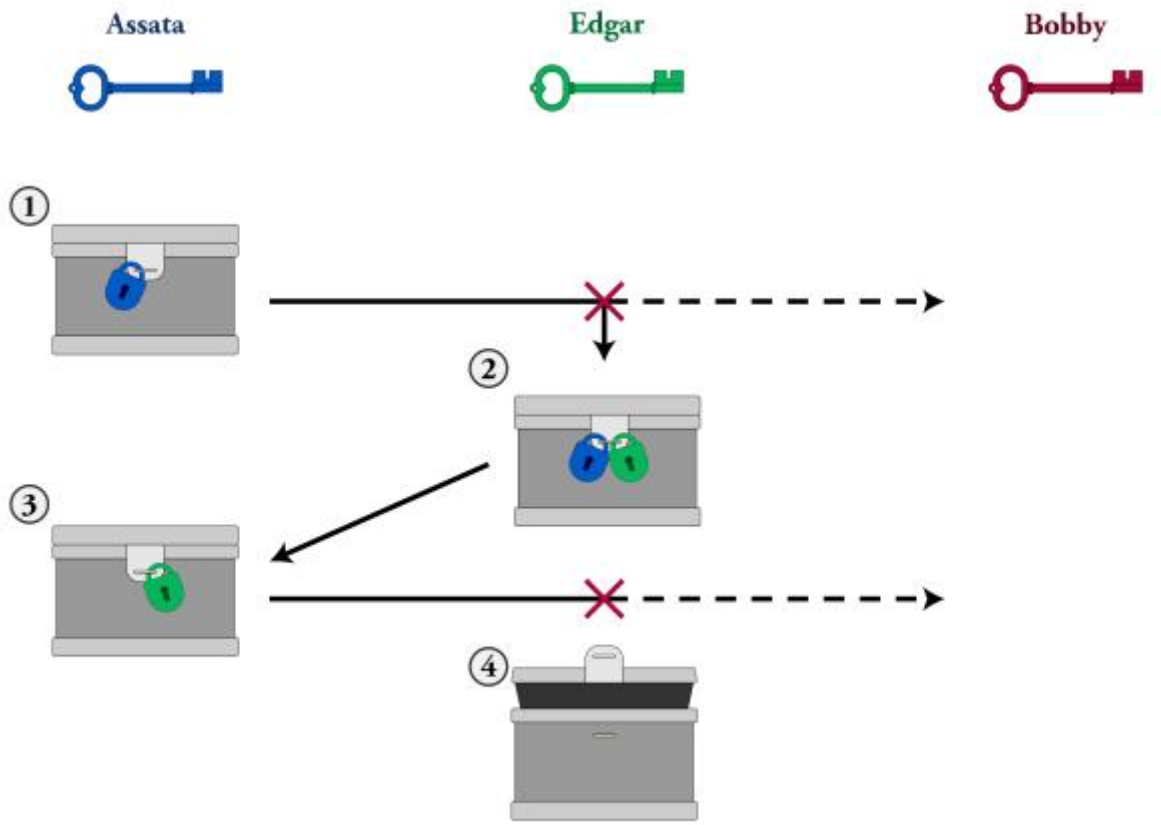
「暗号化のための鍵の交換」の章では、2人の人間が会わなくても、暗号化の鍵に合意する方法を学びました。これは堅牢な方法ですが、インターネット上では、通信しようとしている相手（インスタントメッセージや電子メールを送っている友人や、Webページを読み込もうとしているサーバーなど）が本当に当の本人かどうかを確認するのが難しいという問題があります。ここでは、「暗号化のための鍵の交換」の章で紹介した鍵をかけた箱の例を用いて、盗聴者がどのように通信を傍受するかを説明し、次にディフィー・ヘルマン鍵交換でこのことがどのようになされるのかを説明します。このような通信の傍受は「攻撃」と呼ばれます。

16 (訳注)Earth First! 米国のなかでも有数のラディカルな環境運動団体。https://earthfirstjournal.news
17 (訳注)man-in the-middleを「中間者」と訳している。

物理的な中間者攻撃

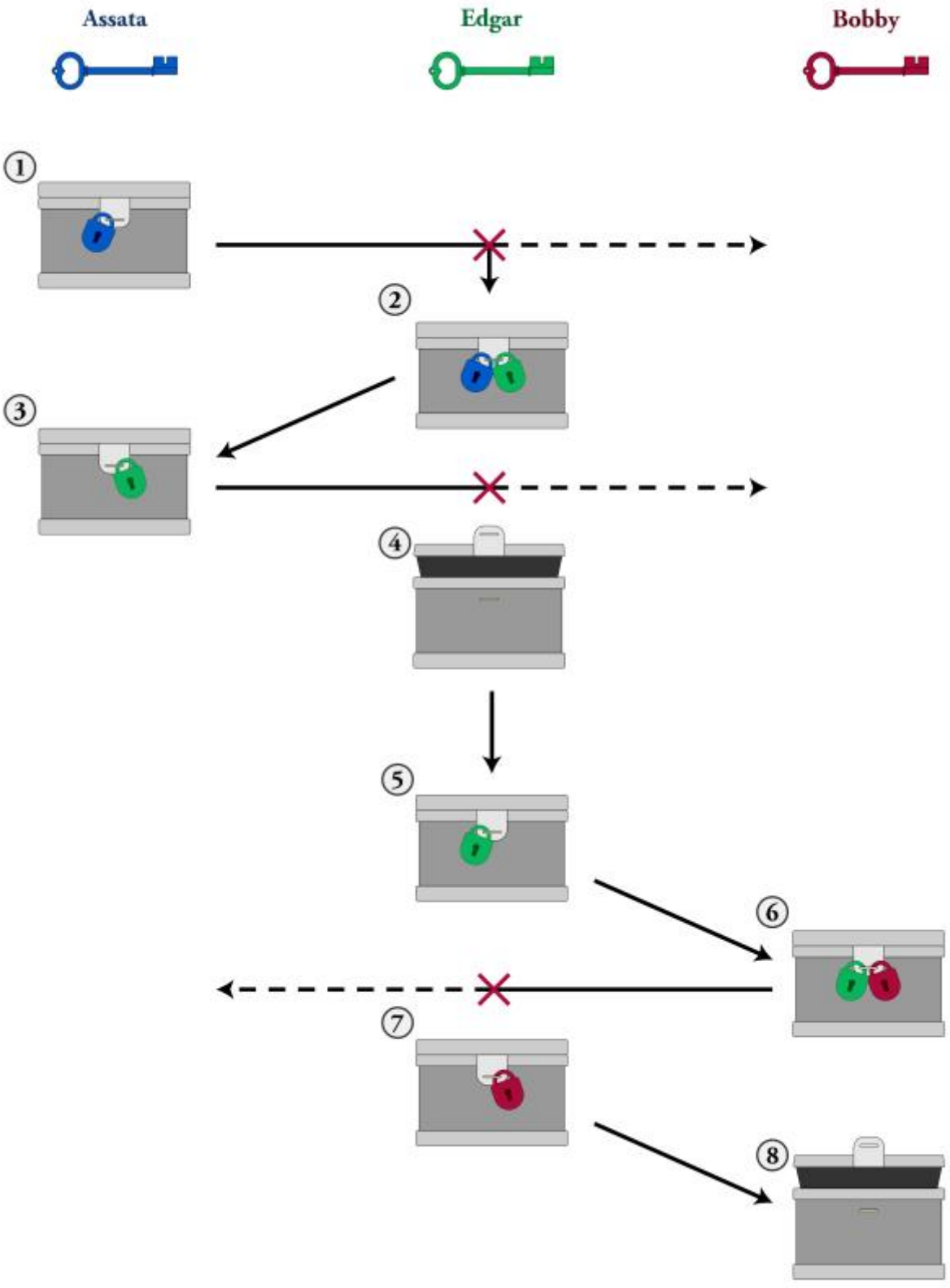
アサタは、鍵のかかった箱を 3 回やりとりすることで、ボビーへ安全にパッケージを送ることができました。1 回目は彼女が施錠した状態、2 回目はボビーが施錠した状態、3 回目は彼女が自分の施錠を外してボビーの施錠だけにした状態です。しかし、この荷物を受け取るのがボビーだということを、彼女はどうやって知るのでしょうか？そして、その箱が彼女に送り返されてきたときに、それがボビーの施錠であることをどうやって知ることができるのでしょうか？

下の図のように、アサタが施錠してボビーに送られる箱をエドガーが横取り(傍受)したとします(1)。エドガーは、自分の施錠した箱をアサタに送り返すことができます(2)。アサタはエドガーの施錠とボビーの施錠の違いを見分けられない限り、アサタは施錠がボビーによるものであると仮定して、自分の施錠を外して、ボビーに箱を送るでしょう(3)。もしエドガーが再び荷物を横取りしたら、今度は自分の施錠だけなので、箱を開けて荷物の中身を調べることができます(4)。こうするためには、エドガーはアサタからボビーに送られてくる荷物をすべて傍受しなければなりません。このような方法でアサタとボビーのコミュニケーションを攻撃することを「なりすまし攻撃 impersonation attack」といいます。エドガーはボビーになりすましているということです。(これは、一般的には中間者攻撃とはみなされません)。



なりすまし攻撃

このような状況では、ボビーは箱をまったく受け取っていません。しかし、エドガーはさらに先を行くことができます (下図)。エドガーは、アサタからの施錠された箱を開封した後(4)、同じ 3 つの交換方法のミラーイメージを使ってボビーに送信し、ボビーがアサタから施錠された箱を受け取ったと思い込ませることができます(5)-(8)。



中間者攻撃

エドガーがアサタのオリジナルのメッセージを（メッセージの内容を確認しただけで）渡した場合、これを受動的な中間者攻撃と呼びます。エドガーが全く別の箱にとりかえた場合は能動的な中間者攻撃です。いずれの場合も、エドガーはボビーとアサタの間のすべて

の箱を傍受する必要があります。なぜなら、箱の宛先はボビーかアサタであって、エドガーではないからです。

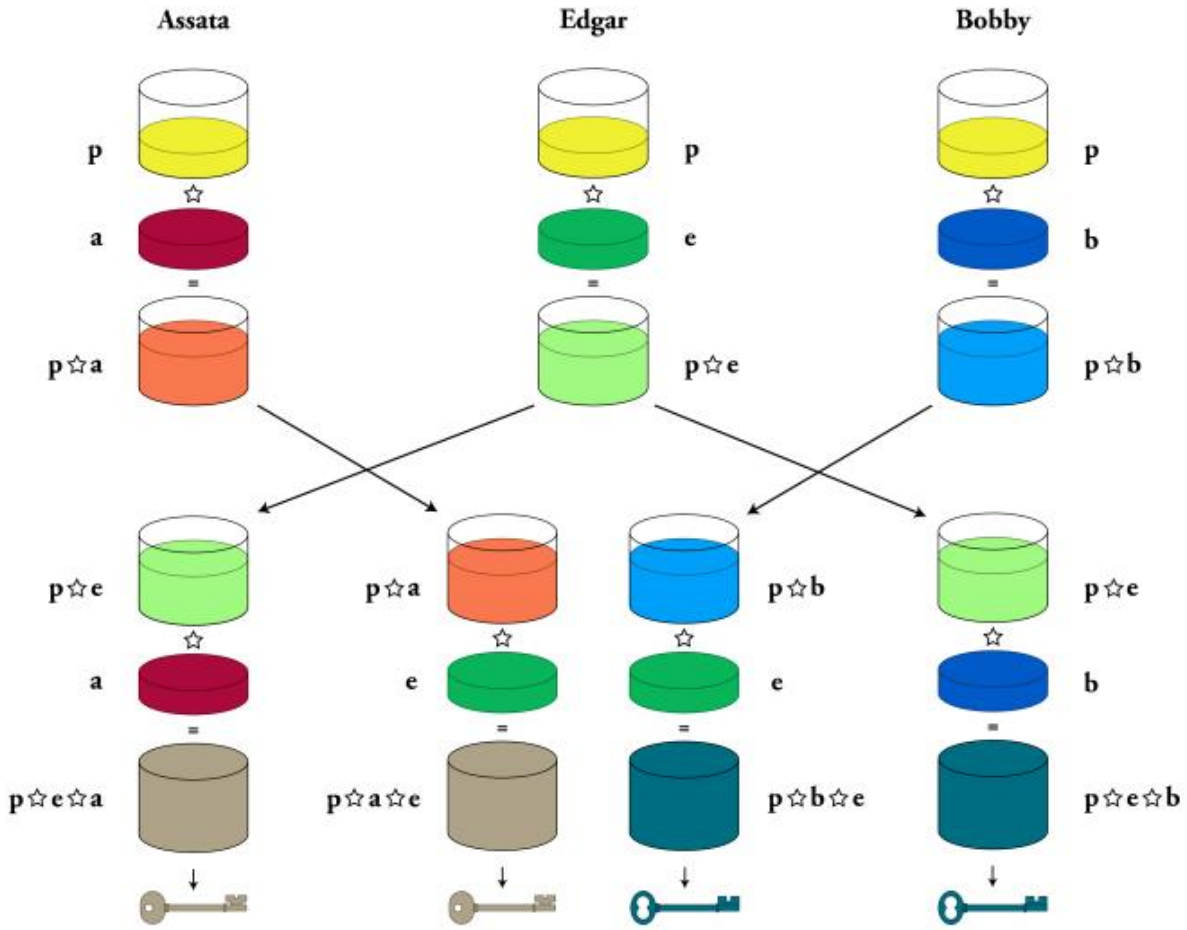
このような攻撃は、エドガーがアサタとボビーの通信の中間にいる者 the man in the middle であることから、中間者攻撃と呼ばれています。(J.エドガー・フーバーの場合は、文字通り「その男 the man」と言われました[18])。

ディフィー・ヘルマン鍵交換に対する中間者攻撃

「暗号化のための鍵の交換」の章で紹介した表記法を使って、Ðiffie-Hellman 鍵交換がどのように行われるか見てみましょう。アサタとボビーが鍵を生成するためには、最初に二人はある数値 p に合意していなければなりません。アサタは数字 a を選び、p☆a を計算し、その結果を ボビーに送ります。ボビーは数字 b を選び、p☆b を計算して、その結果をアサタに送ります。これで アサタとボビーは p☆a☆b を計算することができるようになり(彼ら以外は誰も計算できません)、これを暗号化された通信のための暗号鍵として使用します。

さて、ここでエドガーがアサタとボビーの通信を傍受できたとします。このとき、エドガーはアサタとディフィー・ヘルマン鍵交換を 1 回、またボビーともディフィー・ヘルマン鍵交換を 1 回行うことができます (下図)。アサタはボビーとディフィー・ヘルマン鍵交換をしていると思っていますが、実際にはエドガーと鍵交換をしており、ベージュ色の鍵 p☆a☆e ができます。ボビーはアサタとディフィー・ヘルマン鍵交換をしていると思っていますが、実際にはエドガーと鍵交換をしており、青色の鍵 p☆b☆e ができます。結局、アサタとエドガー左の共有鍵を、エドガーとボビーは右の共有鍵を持っていることになります。しかし、アサタとボビーはお互いの共有キーを持っていると思っています。

18 (訳注)カート・ジェントリーによる評伝『フーヴァー長官のファイル』(吉田利子訳、文芸春秋)の原題は、J. Edgar Hoover, The Man And The Secrets。



ディフィー・ヘルマン鍵交換に対する中間者攻撃

アサタとボビーが共有鍵だと思っているもの(実はエドガーによってすり替えられた偽物)を使い始めたあとも、エドガーはバレないように策略を続けなければなりません。つまり、アサタは自分が持っている鍵でメッセージを暗号化します。このメッセージがボビーに届いたとしても、ボビーは同じ鍵を持っていないので、メッセージを解読することはできません。エドガーがすべきことは、暗号化されたメッセージを傍受し、アサタと共有している鍵で復号することです。ここでエドガーには 2 つの選択肢があります。エドガーは単純にメッセージを読み、ボビーと共有している鍵で暗号化し、ボビーに送信する。これは、受動的な中間者攻撃です。つまり、エドガーはアサタとボビーの間のメッセージを読んでいますが、アサタとボビーは誰にも読まれていないと思っています。エドガーのもう一つの方法は、アサタからのメッセージを変更し、ボビーと共有している鍵で暗号化し、ボビーに送信することです。これは能動的な中間者攻撃です。いずれの場合も、エドガーはアサタとボビーの間の通信を継続的に傍受しなければなりません。そうしないと、どちらかが自分の持っていない鍵で暗号化されたメッセージを受け取ってしまい、中間者の存在が知られてしまうからです。

暗号ハッシュによる中間者攻撃の発見 フィンガープリンティング

アサタとボビーがディフィー・ヘルマン鍵交換を行った後、2 人の鍵を比較して同じ鍵であることが確認できれば、盗聴者が中間者攻撃を行っておらず、2 人だけが暗号化された通信を見ていることが確認できます。この理由は、ディフィー・ヘルマン鍵交換の一部を盗聴者が見ても、アサタとボビーがそれぞれ選択した鍵の隠された部分 (上の図の a と

b) を作ることはできないからだということを思い出しましょう。実際、中間者攻撃を発見する最も基本的な方法は、アサタとボビーがそれぞれの鍵を比較することです。

この方法にも、問題があることにお気づきでしょう。

つまり、アサタとボビーが鍵を比較しようとした場合、エドガーが通信を操作して、鍵が同じであるかように見せかけたりしないでしょうか？

もちろんこれは可能です。そこで、アサタとボビーは別の通信手段で鍵を比較すべきだということになります。たとえば、もともとインターネットで通信していたのであれば、電話でキーを比較するのです。これは、鍵を比較するためのアサタとボビーのあらゆる通信をエドガーが傍受するのは極めて困難だという前提に立っています。理想的には、アサタとボビーが直接会ってキーを比較することです。いずれにしても、これは帯域外比較 out-of-band comparison と呼ばれます。帯域 band とは通信チャネルのことで、鍵の比較は、鍵が交換される通信の帯域とは別に行われるべきなのです。

しかし、ちょっと待ってください。もしアサタとボビーが別の通信手段を持っているのなら、複雑な計算をせずに昔ながらの方法で、鍵を交換すればいいのではないでしょうか？

そうなのですが、最近の暗号方式の鍵は、数百文字から数千文字という非常に長いものになっています。コンピュータを使わずに鍵の交換をするのは面倒です。もし、安全な通信手段の設計者が、別の通信チャネルで鍵の交換を自動化しようとすると、その別の通信チャネルを指定しなければならず、安全な通信システム全体が煩雑になってしまいます。(Web サイトにアクセスするために電話をかけなければならないことを想像してみてください。)また、エドガーはどのチャネルで鍵が交換されているかを察知すれば、そのチャネルでも中間者を演じることができます。

それにしたって、そんなに長い鍵を比較するのは面倒でしょう？

そうですね。そこで、アサタとボビーは、鍵全体を比較するのではなく、「暗号化ハッシュ」の章で説明したように、鍵の暗号化ハッシュを比較します。以下の暗号化ハッシュの性質を思い出してください。(1)入力 (ここでは鍵) が長くてもハッシュは非常に短くなる (例えば数十文字程度) 。(2)出力ハッシュが同じになるような 2 つの異なる入力 (ここでは 2 つのキー) を見つけることはほとんど不可能ですから、エドガーは、ハッシュが同じになるようにアサタとボビーとの間でディフィー・ヘルマン鍵交換を操作することはできません。(3) もし誰かがハッシュを傍受しても、そこから入力 (この場合は鍵) を再度生成するといったリバースはできません。

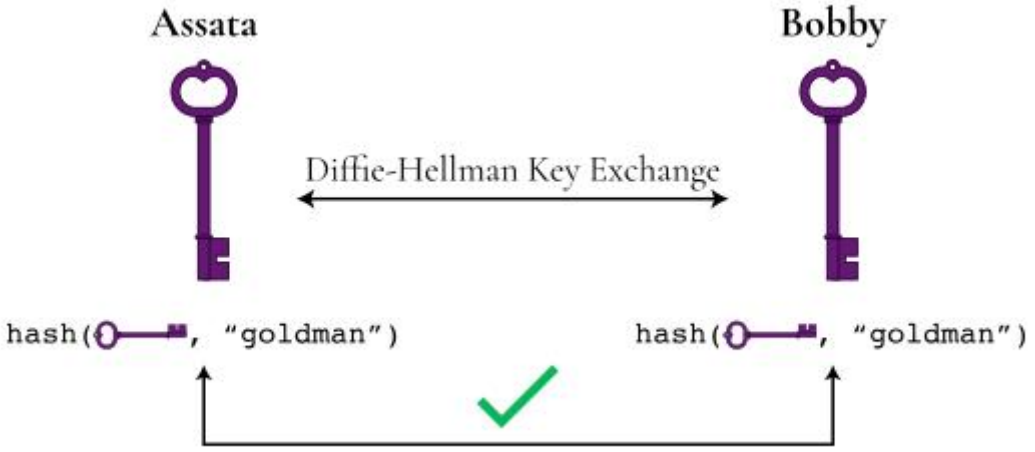
なお、暗号化ハッシュをフィンガープリント(指紋)と呼ぶことがあるので、鍵の暗号化ハッシュを比較することをフィンガープリンティングと呼ぶことも思い出してください。フィンガープリンティングは安全番号(safety numbers)、検証(verification)、認証(authentication)など、アプリによって違う用語が使われている場合があります。

帯域内フィンガープリンティング

帯域内で鍵を比較する方法には、一般的にはあまり使用されていないけれど巧妙な方法が 2 つあり、どちらも前述の帯域外フィンガープリンティングのバリエーションです。

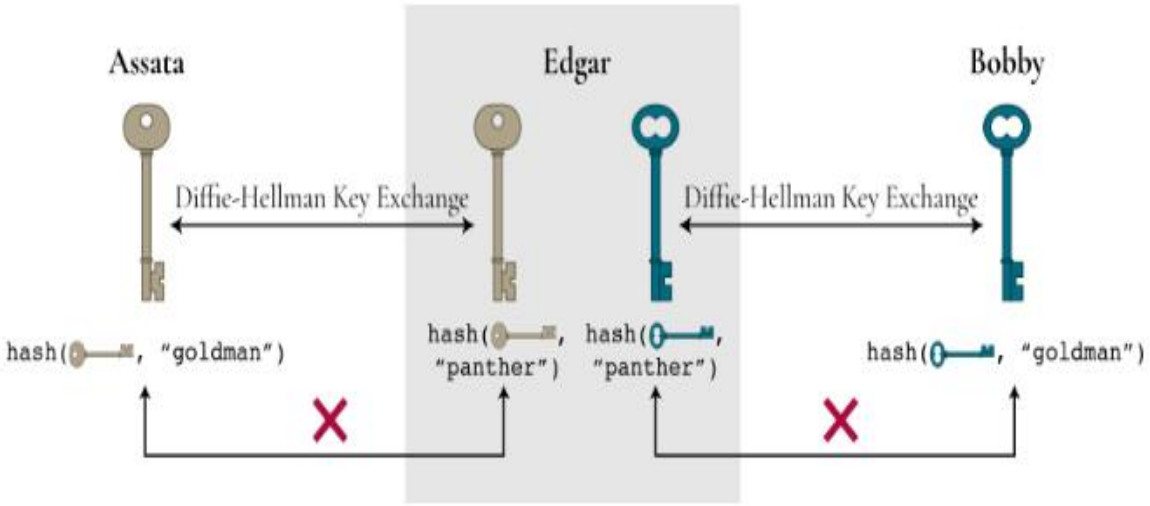
1 つ目の方法は、弱いパスワードを使用するものです。アサタの最初のペットの名前やボビーの生家の地名 (例えば「ゴールドマン通り」) など、敵が知らないことをアサタとボビーが知っていれば、アサタとボビーはこれを弱いパスワードとして使うことができます。アサタは自分の鍵と弱いパスワード (″ゴールドマン通り″) を組み合わせて、その結果の暗号化ハッシュを計算します。ボビーは自分の鍵で同じ計算をする。アサタとボビーは、

その結果を既に通信している通信チャネルで比較します。暗号化ハッシュの性質上、アサタとボビーは同じ鍵と同じパスワードを持っている場合にのみ、同じ結果になります。



フィンガープリンティング

エドガーが中間者を演じている場合、エドガーはアサタと鍵を共有し、ボビーとは別の鍵を共有しています。エドガーはバレるリスクを承知でアサタのハッシュをそのままボビーに渡すか、または、アサタが計算する結果とボビーが計算する結果を同じにするためにその弱いパスワードを推測しなければなりません（下図）。アサタとボビーの間では、パスワードが強固である必要はありません。エドガーが推測を一度でも失敗すると（例："panther"）中間者攻撃の存在がわかってしまうので、エドガーはブルートフォース攻撃でパスワードを推測するわけにいかないのです。



中間者攻撃を発見するためのフィンガープリンティング

2つ目の方法は、音声通話やビデオ通話を使った鍵の比較に用いられます。ここでは、アサタは自分の鍵を、（これまで見てきたような数字や文字の羅列ではなく）人間が読める2つの単語にハッシュ化します。ボビーも同じことをします。アサタとボビーが同じ鍵を持っていれば（つまり、中間者がいなければ）、2人は同じ単語を共有することになります。アサタは最初の単語を読んでボビーへ伝え、ボビーは2番目の単語を読んでアサタへ伝え、それぞれがハッシュの結果を比較できます。もしエドガーが中間者を演じていれば、アサタとボビーは2つとも別々の単語を持つことになります。エドガーが策略を続けるた

めには、エドガーはアサタとボビーが共有している 2 つの単語を話すために、アサタとボビーの声（場合によってはビデオも）を合成しなければなりません。

フィンガープリント認証は、全員がやらなくても保護になる

安全な通信手段があっても、鍵の比較（フィンガープリント）ができなければ、エンド・ツー・エンドの暗号化を使用するメリットはほとんどありません。中間者攻撃は世界的な監視システムでは自動化されているので、中間者攻撃の実態を（フィンガープリントによって）見抜けないのであれば、いつでも中間者攻撃が実行されていると見なすべきです。ところが、フィンガープリントが可能な場合、特に攻撃が自動化され広く行われている場合には、中間者は発見されてしまうリスクがあります。一部のユーザーがフィンガープリントのプロセスを経ていれば、全員がフィンガープリントを行わなくても中間者攻撃の広がりを防ぐことができるのです。

もちろん、対象を限定した監視にさらされるリスクがあるユーザーにとっては、通信の安全性を確保するためにフィンガープリントは不可欠です。

フィンガープリントができないときの対処法

フィンガープリンティングができない通信手段もたくさんあります。例えば、ウェブサイトに https でアクセスする場合です。https では、ブラウザと Web サイトのサーバーとがディフィー・ヘルマン鍵交換によって暗号鍵を生成します。しかし、ユーザーが Web ページのコンテンツにアクセスする前に、別の通信手段で Web サイトのサーバーに連絡を取り、鍵のフィンガープリントを取得することは現実的ではありません。というのも Web サーバの電話オペレータの声を知っているわけでもないし、帯域内比較を使うための知識をもっているわけでもありませんから。このような場合には、公開鍵暗号方式や認証局を利用した別の鍵の検証方法が用いられます。公開鍵暗号方式については、「公開鍵暗号方式」の章で説明します。

コンテクスト：中国のグレート・ファイア・ウォール

中国では、"グレート・ファイア・ウォール"によってインターネットが厳しく検閲されていることは多くの人が知っています。2013 年 1 月中旬から、主にコンピュータのプログラミングコードのホスティングに使用され、さらに一般的な情報共有にも使用されているサイト、GitHub の一部が中国でブロックされました。2013 年 1 月 21 日には、ドメイン全体がブロックされました。しかし、GitHub がコンピュータの開発やビジネスで中心的な役割を果たしていることや、この分野が中国経済にとって重要であることを考慮し、世論の反発を受けて、2013 年 1 月 23 日までに GitHub のブロックは解除されました。1 月 25 日には、WhiteHouse.gov で、グレート・ファイア・ウォールの構築に関与した人々の米国入国を拒否するよう求める請願書が作成されました。この請願書は、同じ日に作成された、中国の検閲インフラに貢献したとされる中国人のリストをアップした GitHub ページにリンクされていました。その翌日には、GitHub にアクセスするユーザーが中間者攻撃を受け、https 経由で Web サイトにアクセスする際のフィンガープリント認証に相当するチェックが失敗したという報告がソーシャルメディアに掲載されました。中国政府は、GitHub をブロックできないことを知っていました。またグレート・ファイア・ウォールでは、キーワードの一致などを利用しても、GitHub 内の特定のページへのアクセスだけをブロックできないのです。というのも GitHub が https に対応しているため、https で暗号化して盗聴者から守っているからです。そこで次の方法が、中間者攻撃です。ユーザーが攻撃の警告サインを無視すると、どのページにアクセスしているのか、あるいは編集しているのかを政府に知られてしまう危険性があります。中国政府は、中国国内のユーザー

と、Outlook、Apple の iCloud、Google などの主要なインターネットサービスとの間で広範な中間者攻撃を展開していると推定されています。

中間者攻撃を行っているのは中国だけではありません。シリアやイランでも同様の攻撃が見つかっています。

次に学ぶこと

コミュニケーションを守るために

外部リソース

・GreatFire は、中国の無検閲インターネットにアクセスするためのツールを提供し、中国のインターネット検閲や監視を報告・検証しています。特に GreatFire は、Outlook、Apple の iCloud、Google、GitHub に対する、中国政府によるものと思われる中間者攻撃を報告・検証しています。

・Eckersley, Peter. “A Syrian Man-in-the-Middle Attack against Facebook.” Electronic Frontier Foundation, May 5, 2011.

・電子フロンティア財団. “Iranian Man-in-the-Middle Attack against Google Demonstrates Dangerous Weakness of Certificate Authorities.”. August 29, 2011.

図版の出典

なりすまし攻撃 mitm-impersonation © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

中間者攻撃 mitm © OSU OERU は CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

ディフィー・ヘルマン鍵交換に対する中間者攻撃 dhe-mitm © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

フィンガープリンティング fingerprinting © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

中間者攻撃を発見するためのフィンガープリンティング fingerprinting-mitm © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

パスワードについて

この章を読む前に、「暗号化ハッシュ」の章を読むことをお勧めします。

この章で学ぶこと

1. 「パスワード保護」が暗号化を意味する場合とそうでない場合
2. パスワードはどのように破られるのか
3. パスワードのリスクを最小限に抑えるためのパスワードの使い方
4. パスワードから暗号化キーを生成する方法

「パスワード保護」が暗号化を意味しない場合

パスワードはアクセスを制御するために使用されます。例えば、オンラインアカウントへのアクセスを許可するためにアカウントパスワードが使われます。しかし、そのアカウント内の情報が自分の管理する鍵で暗号化されているのは稀であり、情報がまったく暗号化されていないこともあります。その場合、プロバイダー（Google や Ðropbox など）はその情報を読み取ることができます。その他のパスワードは、暗号化されたファイルや文書のロックを解除するために使用され、これらを暗号化パスワードと呼ぶことにします。アカウントのパスワードは、予約制の店に入るときに、入口の係に自分の名前を伝えて、その名前と予約客リストの名前と一致させるようなものですが、暗号化パスワードの使用は、金庫の錠を開けるために鍵を使うようなものです。前者の場合は、入口の係（あなたが契約しているプロバイダーのたとえ）があなたのアクセスを許可するかどうかに関係しています。後者の場合、金庫が暗号文を表し、金庫の中身が平文です。平文にアクセスするには、鍵やパスワードがなければ不可能です（少なくとも現実的ではありません）。後述するように、暗号鍵はパスワードから生成される場合もあります。

つまり、あなたの情報がアカウントパスワードで暗号化されていなくても、あなたの情報にアクセスできる人数を最小限にすべきなのです。しかし、私たちがなぜこのようなパスワードの使い方を推奨しているかを理解するには、パスワードがどのようにして侵害されるのかを理解する必要があります。

パスワードのクラッキング

パスワードは侵害されることがあります（クラックされる、ともいいます）。あるシステムにあるすべてのアカウントのパスワードが一括して侵害されることもあれば、1 つずつ侵害されることもあります。パスワードは人気商品にも似たところがあって、同じパスワードをあちこちのアカウントで使っている人も多いし、「人気のある」パスワード（ひどいパスワードともいいますが）は多くの人々に利用されています。(たとえば 123456、password、qwerty、admin、welcome など）。もしあるサービスで使われているパスワードが露見してしまうと、別のサービスや別の人のアカウントが侵害される可能性があるのです。

パスワードがどのように侵害されるかを考えてみましょう。

パスワードをひとつ解読するために敵が使う手段は、あなたがパスワードを入力するときと同じです。例えばウェブサイトを介してパスワードを破ることができます。この場合、ウェブサイトの管理者は、比較的簡単にパスワードを保護することができます。例えば、数回パスワードを間違えたらアカウントをロックしたり、パスワードを入力した後はサーバーの反応を強制的に遅らせて、繰り返して入力することによる推測を防いだりします。アカウントの管理者ができるもう一つの方法は、二要素認証を可能にすることです。二要素認証とは、アカウントにアクセスするためにパスワードを入力することに加えて、SMS やスマートフォンのアプリ、または物理的な認証キー（YubiKey など）へ送られてくる認証コードの入力も必要とするものです。アカウントを侵害するために、敵はパスワードだけでなく、認証コードを受け取るデバイスも必要になるのです。

敵は、あなたがパスワードを入力したデバイス（携帯電話やコンピュータ）に物理的にアクセスすることもできます。でも、より可能性が高いのは、ニュースでよく報道されているように、あなたのパスワードが保存されているサーバーが侵害されたり、ハッキングされたりすることです。この場合、あなたのユーザー名とパスワードだけでなく、そのシステムにアカウントを持つすべての人が危険にさらされることになります。サーバー上のパスワードデータベースにアクセスした敵は、あなたのアカウント情報にもアクセスできる可能性がありますが、上述したように、ハッキングの目的は、ハッキングされたサービスではなく、もっぱら別のサービスへのアクセスを得るのが目的かもしれません。

責任あるウェブサービスプロバイダーは、パスワードを平文でサーバーに保存せず、パスワードの暗号化ハッシュを保存します。こうしておくと、1個のパスワード（またはすべてのパスワード）を発見するために、敵はパスワードを推測し、その暗号ハッシュを計算し、これを盗んだパスワードのデータベースと比較します。実際には、パスワード推測ツール（John the Ripperなど）は以下の3つの手法を使います。

1．辞書攻撃：辞書の単語、少しひねった辞書の単語（例：pa55w0rd、fr33d0m）、および以前にクラックされたパスワードを試す。[19]

2．ブルートフォース：ありうる限りの文字や記号の組み合わせを全部試す（実用上の理由から、この方法は比較的短いパスワードにしか使えない）。

3．事前に計算されたハッシュ：あらかじめパスワード候補と暗号ハッシュの表を作っておいて、それと比較する。

ユーザーは、後述する適切なパスワード管理を行うことで、最初の2つの手法を回避することができます。サービスプロバイダーは、計算に時間がかかる、あるいは大量のメモリを使用する暗号ハッシュ関数を使用することで、パスワードのクラッキングを実用的でないものにすることができます。この手法は、ログイン時などで単一のパスワードについて行なわれるとき気にならないかもしれませんが、クラッキング時にはハッシュの計算が遅くなります。

サービスプロバイダーは、ログイン時のパスワードに長いランダムな文字列（ソルト）を追加することで、事前に計算されたハッシュの使用をさらに妨げることができます。このソルトは、ユーザー名と一緒に平文で保存されることもあるため、敵はこの情報も把握するかもしれませんが、事前の計算でハッシュの表を作成する時点ではソルトを持っていなかったことでしょう。さらに、2人のユーザーが同じパスワードを使っている場合でもソルトが異なるため、それぞれのソルトを使えばパスワードの暗号ハッシュも異なります。このため、攻撃者はそれぞれのパスワードを個別に暴かなければなりません。

あなたはオンラインサービスの管理者が責任を持ってあなたのユーザー情報を保管し、ときには暗号化ハッシュも用い、このような攻撃から保護していると信頼することにします。次はあなたの番です。

パスワードのベストプラクティス

パスワードクラッキングの手法に対抗するためには、パスワードは十分な長さで（ブルートフォース攻撃を防ぐため）、一般的単語でなく（辞書攻撃を防ぐため）、しかも再利用されていないもの（1つのアカウントが侵害されても、他のアカウントが侵害されないため）が必要です。

これを実現するには、手動で入力しなくてもよいところでは、パスワードマネージャーを使ってパスワードを生成し、保存します。パスワードマネージャーは、bdY,Fsc_7\&*Q+cFPのような強力なランダムパスワードを生成することができるはずです。これは、手動で入力しなくてもよいとき、つまり、パスワードマネージャーがあなたに代って入力してくれるパスワードとしては最適です。

必ず入力しなければならないパスワード（携帯電話で入力するパスワード、パスワードマネージャーを保護するためのパスワード、コンピュータの暗号化やロック解除に使用する

19 (訳注)原文では salt と表記。ソルトには次段の説明にもあるように認証システムがパスワードなどを保存する際に付け加えるランダムな符号列の意味がある。https://e-words.jp/w/%E3%82%BD%E3%83%AB%E3%83%88.html

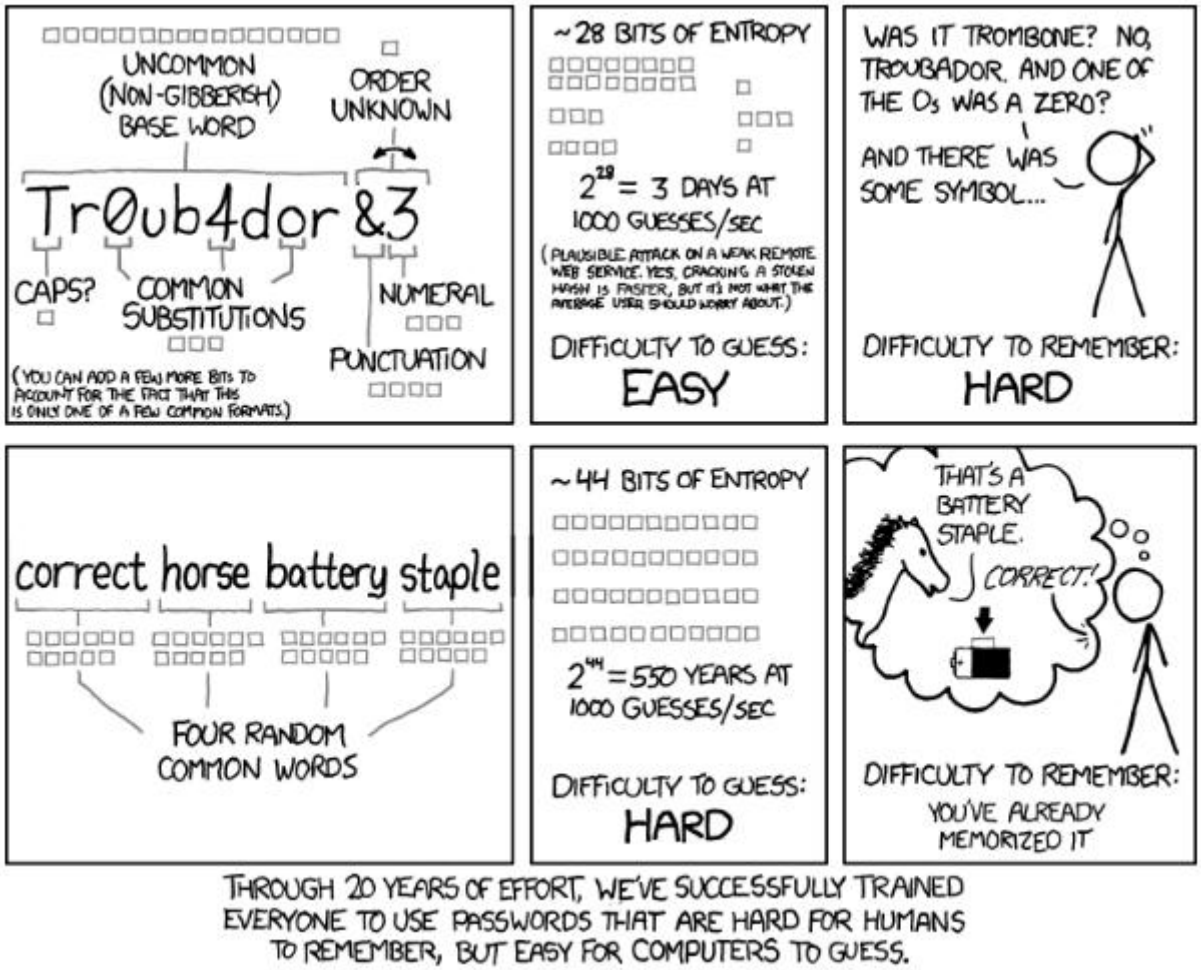
パスワードなど）には、次のようなランダムな単語の羅列である「ダイスウェアパスワード」（パスフレーズ）[20]を使用してください。

remake.catfight.dwelled.lantern.unmasking.postnasal

このパスワードは、サイコロと単語リストを使って手動で生成することができます。おおかたのパスワードマネージャーでも生成できますが、どちらにせよこのパスワードはそれほどたくさん必要となるものではありません。

上の 2 つの例でパスワードはランダムに生成されていることに注意してください。これは重要なことです。自分で作ったパスワードが素晴らしく強力だと思えても、あなたの脳で考えたものなら、おそらく他の誰かの脳でも考えることができるでしょうから、辞書攻撃の影響を受けやすいのです。

人間には覚えにくくて、コンピュータなら簡単に当てられるようなパスワードを、かれこれ 20 年もかけて宣伝してきたわけです。



XKCD のパスワード強度

パスワードから暗号化キーを生成する

20(訳注)「ダイスウェア（Diceware）とは、ダイス（さいころ）を使って「ダイスウェア単語一覧」と呼ばれる単語一覧から単語をランダムに選び、パスフレーズを作る方法のことである。」https://www.hyuki.com/diceware/ あるいは、https://www.rempe.us/diceware/#eff

暗号化されたファイルやデバイスを解除するために使うパスワードがあります。実際にこの場合は暗号化キーが鍵導出関数という暗号化ハッシュ関数を使用して、パスワードまたはパスフレーズから生成されます。暗号ハッシュ関数の入力はパスワードであり、出力は暗号鍵です。なぜこのようなことができるのでしょうか？暗号ハッシュ関数の特性を再確認してみましょう。

1．入力の長さにかかわらず、出力は常に同じ大きさです。つまり、どんなに短い（そして弱い！）パスワードでも、適切なサイズの暗号鍵を得ることができます。(ただし、短くて弱いパスワードは、上で説明したパスワードクラッキングの手法で破られやすい)

2．同じ入力は、常に同じ出力になります。つまり、あなたのパスワードは常にあなたが必要とする対応する暗号鍵を生成します。

3．出力から入力を生成することは不可能です。ですから、もし誰かがあなたの鍵を手に入れたとしても、少なくともあなたのパスワードを再現することはできません。

4．同じ出力になる2つの異なる入力を見つけることはできません。そのため、あなたのパスワードを解読しようとする人は、あなたのパスワードと同じ暗号鍵を生成する別のパスワードを見つけることさえできないでしょう。

5．入力を少し変えると出力が大きく変わり、新しいハッシュ値が古いハッシュ値と無相関に見えること。まあ、この性質は暗号鍵の生成にはあまり役立ちませんが…。

コンテクスト： 対策が破られるとき

2016年、長年の活動家であるデレイ・マッケソン ĐeRay Mckessonは、2要素認証[21]を設定していたにもかかわらず、標的攻撃を受けて自分のTwitterアカウントと2つのメールアドレスが侵害されました。敵は、ベライゾンに電話して新しいSIMカードを要求することで彼の携帯電話をコントロールすることができました。敵は、ベライゾンを説得できるほどマッケソンのことを知っていたのです。敵はマッケソンの電話番号でサイトにアクセスすると、パスワード再設定コードを受け取り、マッケソンのパスワードを変更して、マッケソンのアカウントにアクセスできるようになりました。これは、完璧なセキュリティ対策は存在しないこと、従って、標的となりうる人（今回の場合、マッケソンはBlack Lives Matterを支持していたために標的となった）には、特別な警戒が必要であることを示しています。マッケソンの電話番号を使ってパスワードをリセットすると2要素は解除されて、アカウントの保護は1要素だけになりました。マッケソンのアカウントを敵から守っていたのはパスワードと電話とによる認証ではなく、電話だけだったのです。

次に学ぶこと

・公開鍵暗号方式[22]

外部リソース

Đreyfuss, Emily. “@Đeray’s Twitter Hack Remind Us Even Two-Factor Isn’t Enough.” Wired, June 10, 2016.

ウィキペディア。”John the Ripper(英語)” 2020年12月29日版。

TeamPassword. “2019年のワーストパスワードトップ50(英語)” 2019年12月18日版。

---

21 （訳注）利用者の本人確認などの認証において、二つの異なる原理の認証手段を組み合わせて用いることにより精度と安全性を高める手法。パスワードとSMSなどで送信されるワンタイムパスワードの組み合わせなどがこれに該当する。(IT用語辞典)

22 原書では「デバイスの保護」となっているが、訂正した。

図版の出典

XKCD のパスワード強度 password_strength © Randall Munroe is licensed under a CC BY-NC (Attribution NonCommercial) license

公開鍵暗号方式

この章を読む前に、「暗号化のための鍵の交換」の章を読むことをお勧めします。

この章で学ぶこと

1．対称鍵 symmetric-key 暗号[23]方式と非対称暗号 asymmetric-key の違い

2．公開鍵暗号方式のメカニズム

暗号化方式は大きく 2 つ別けられます。一方の対称鍵暗号では暗号化の鍵と復号する鍵とが同一(または容易に暗号鍵から変換できる鍵)です。「暗号化とは何か？」の章で紹介した基本的な暗号 (シーザー、ヴィジュネル、ワンタイムパッド) がこの仲間です。(携帯電話やパソコンのデータの暗号化に使用される最新の対称鍵暗号もあります。)しかし、これらの暗号では通信相手と秘密裏に鍵を共有する必要があるため、通信で使用するのはやや難しいのです。ディフィー・ヘルマン鍵交換は、2 人の人間がインターネットなどの安全ではない経路でのみ通信しながらも、共有の鍵を生成して対称鍵暗号化方式を使えるようにする方法です。

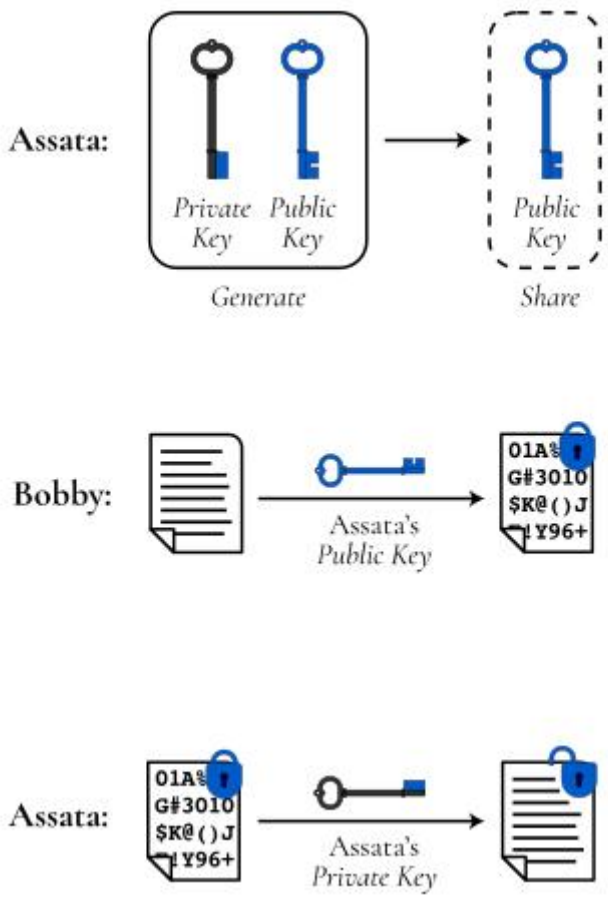
他方の非対称鍵暗号方式 (公開鍵暗号方式) は、鍵の共有問題を別の方法で解決しています。公開鍵暗号方式では、1 つの鍵を暗号化と復号の両方に使うのではなく、暗号化の鍵 (公開鍵と呼ばれる) と復号の鍵 (秘密鍵[24]と呼ばれる) の 2 つの鍵を使用します。この 2 つの鍵は次のような性質を持っています。

1．公開鍵から秘密鍵を生成することは不可能であり、2 つの鍵はあらかじめ生成しておく必要がある。

2．公開鍵で暗号化されたメッセージの復号は、現実的には対応する秘密鍵でのみ可能である。

ボビーからアサタへ暗号化してメッセージを送りたいとします。アサタはあらかじめ秘密鍵と公開鍵をペアで作成し、ボビーに公開鍵の方を (安全ではない経路で) 送信します。ボビーはその公開鍵を使って暗号化し、暗号文をアサタに送信します。この暗号文はアサタの秘密鍵を使ってのみ復号できるものです。アサタの公開鍵は誰もが持っているにもかかわらず、この公開鍵で、アサタの秘密鍵でしか復号できないような暗号文を作ることができるのです。したがって、秘密鍵を秘密にして保管しておけば、セキュリティが確保されます。

23 (訳注) 共通鍵暗号と呼ばれる場合もある。
24 (訳注)プライベート鍵とも呼ばれる。



公開鍵(Public Key)と秘密鍵(Private Key)をペアで生成し、公開鍵を共有する。公開鍵で暗号化する、秘密鍵で復号する

この方式なら実際に誰でも自分の公開鍵を公開しておくことができます。例えば、アサタは自分の公開鍵をオンラインで公開し、アサタへ暗号文を送りたい人は、送るメッセージを彼女の公開鍵で暗号化します。同様に、ボビーは自分の公開鍵と秘密鍵のペアを作って彼の公開鍵をオンラインで公開しておけば、他の人がボビーに暗号化されたメッセージを送ることができ、ボビーだけが自分の（安全に保管された）秘密鍵で復号できるようになります。

ディフィー・ヘルマン鍵交換の再検討。公開鍵暗号方式か対称鍵暗号方式か？

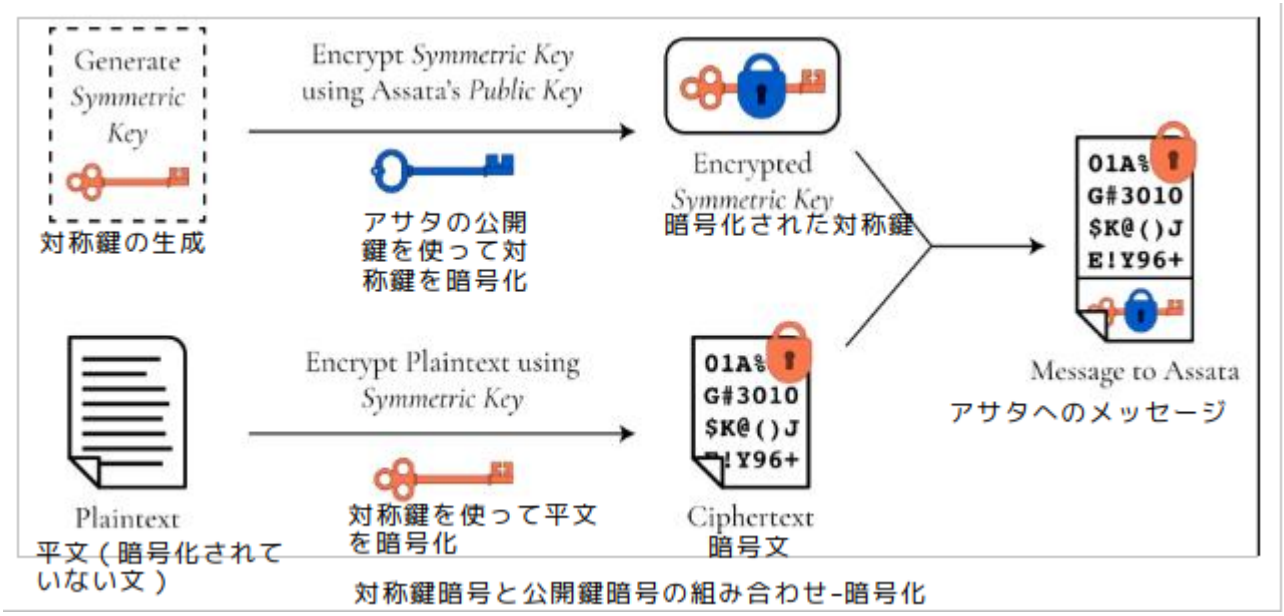
ディフィー・ヘルマン鍵交換について、対称鍵暗号と公開鍵暗号の観点から再度考えてみましょう。アサタとボビーは、ある数pについて（暗号でなく公開で）合意していることを思い出してください。アサタは(秘密)の数字aを選び、p☆aを計算してボビーに(暗号でなく公開で)送信します。この場合、aをアサタの秘密鍵、p☆aをアサタの公開鍵、そしてこの方式を公開鍵プロトコルの一部とみなすことができます。ここでボビーは自分の秘密の数字bを選び、それをアサタの公開鍵と組み合わせて、p ☆ a ☆ bを得ます。同様に、アサタはボビーの「公開鍵」p ☆ bと自分の秘密鍵を組み合わせてp ☆ b ☆ aを得ます。p ☆ a ☆ b = p ☆ b ☆ aなので、アサタとボビーは暗号化に使う共通の鍵を

持ち、復号化にも同じ鍵を使います。このように、これは対称鍵プロトコルの一部です。以上の理由から、ディフィー・ヘルマン鍵交換は、公開鍵暗号と対称鍵暗号の中間に位置するものといえます。

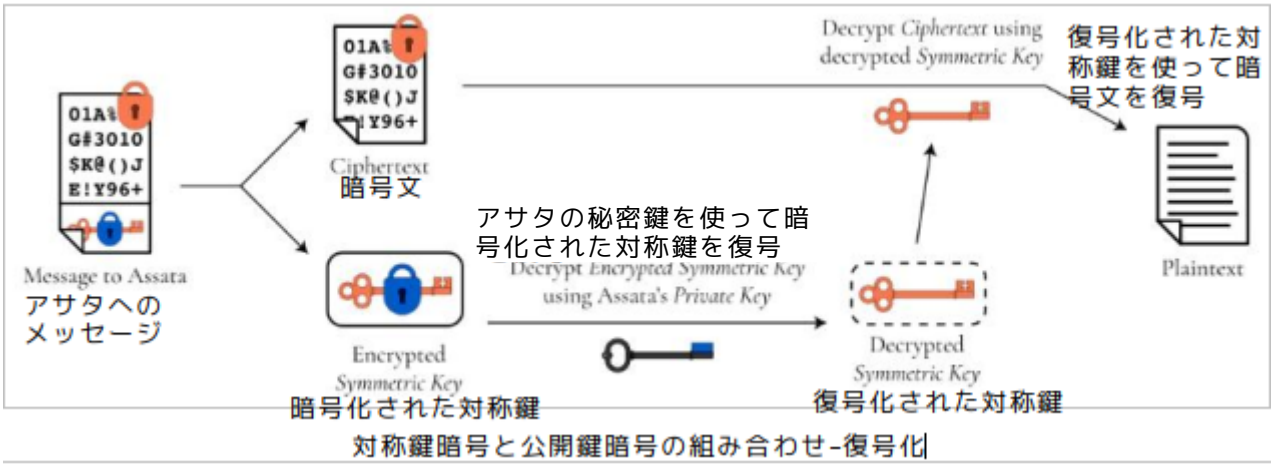
公開鍵暗号方式と対称鍵暗号方式の組み合わせ

公開鍵暗号は通常、対称鍵暗号よりもコンピュータの負担が大きくなります。ブルートフォース攻撃などに対して、対称鍵と同等のセキュリティを実現するには、公開鍵は対称鍵よりもはるかに長い鍵が必要になります。また、暗号化の実行自体も、公開鍵の方が対称鍵よりも時間がかかります。さらに、ある鍵を使って暗号化する期間が長くなればなるほど暗号文が増えていき、ブルートフォース以外の方法で暗号を破ろうとするときの材料を増やしてしまうという問題もあり、鍵が「経年劣化」しやすいのです。

このような理由から、通信セッションでは公開鍵は、対称鍵を暗号化するのに使用されるのが一般的です。例えば、ボビーがアサタに暗号化されたメッセージを送りたいとします。ボビーは対称暗号鍵を生成し、対称暗号を使ってメッセージを暗号化します。その後、アサタの公開鍵を使って対称鍵を暗号化します。そして、暗号化されたメッセージと暗号化された鍵をアサタに送ります。



アサタは自分の秘密鍵を使って暗号化された鍵を復号化し、その結果を使って暗号化されたメッセージを復号化します。



公開鍵は、鍵（一般的にはランダムに見える文字列）の暗号化にのみ使用されるため、人間の言語のフレーズに頼った暗号化の解読方法では失敗するため、公開鍵が古くなることはありません。また、あるメッセージの解読に成功しても、別のメッセージの暗号を解くのには役立たないという利点もあります。なぜなら、それぞれのメッセージは異なる鍵で暗号化されているからです。

コンテクスト 反核活動と Pretty Good Privacy

公開鍵暗号の中でも特に強固に実現されているのが PGP です。これは、謙遜表現である Pretty Good Privacy の頭文字をとったものです。PGP と相互運用可能なフリーのオープンソース版は GPG（GNU Privacy Guard）です。PGP 暗号化の使用をサポートするいくつかのプラグインやメールクライアントを使用して、電子メール通信の暗号化に PGP は最も一般的に使用されています。PGP 公開鍵のオンライン・ディレクトリ（互いに同期されている）がいくつかあり、それぞれが電子メールアドレスと関連付けられているので、ボビーはアサタの PGP キーを調べて、暗号化された電子メールを送ることができます。

長年反核活動家でもあったフィル・ジマーマンが 1991 年に PGP を開発したのは、考えを共有する人たちが掲示板サービス（BBS、1980 年代の Reddit）を安全に利用し、メッセージを安全に保存できるようにするためでした。PGP は、オープンソースのプロジェクトとして開発され、非営利目的の使用にはライセンスは必要ありませんでした。当初は、平和運動を中心とした草の根の政治団体向けのニュースグループに投稿していましたが、ソースコードを配布するためのニュースグループにも投稿され、瞬く間に米国外にも広がりました。ユーザーや支持者には、全体主義国の反体制派、市民的リバタリアン、サイファーパンクなどがいました。しかし、当時、41 ビット以上の鍵を使った暗号システムは、米国の輸出規制の定義では軍需品とみなされていました。PGP は当初、128 ビットの鍵をサポートするように設計されていました。1993 年 2 月、ジマーマンは“無許可の軍需品輸出”の容疑で、アメリカ政府の正式な捜査対象となりました。これに対してジマーマンは、PGP のソースコードをすべて本にして公開し、広く配布・販売しました。PGP を自作したい人は、表紙を外しページを切り離し、OCR プログラムでスキャンすると、ソースコードのテキストファイル一式ができあがります。軍需品（銃、爆弾、飛行機、ソフトウェア）の輸出は制限されていましたが、書籍の輸出は米国憲法修正第 1 条によって保護されています。数年後、ジマーマンの捜査は、彼や他の誰に対しても刑事責任を問うことなく終了しました。

米国の暗号技術に関する輸出規制は、現在も有効ですが、1990 年代後半に大幅に緩和されています。PGP 暗号は、もはや輸出できない武器の定義には当てはまりません。

次に学ぶこと

暗号化“署名“による真正性の確認

外部リソース

電子フロンティア財団 “A Ðeep Ðive on End-to-End Encryption: 公開鍵暗号化システムの仕組みとは？” Surveillance Self-Ðefense, September 29, 2014. (日本語)

Zimmermann, Phil. “Why I Wrote PGP.” 1999.(日本語)

図版の出典

公開鍵暗号: 鍵ペアの生成と公開鍵配布 pubkeycrypto-key-gen-share © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

対称鍵暗号と公開鍵暗号の組み合わせ- pubkeycrypto-split1-encrypt © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

対称鍵暗号と公開鍵暗号の組み合わせ-復号化 pubkeycrypto-split2-decrypt © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

暗号化された署名による真正性(authenticity)

本章をお読みになる前に、「暗号化ハッシュ」と「公開鍵暗号方式」の章を読まれることをお勧めします。

この章で学ぶこと

1. デジタルで署名と同等の機能を実現する方法
2. 暗号化された署名で、どのように真正性が保証されるのか
3. 電子的な真正性とは何か
4. 暗号化された署名を使用すると、どのように“信頼“を広めることができるのか

公開鍵暗号システムは、しばしば真正性の確認に使用されます。PGP では、公開鍵と秘密鍵の相補的な性質を利用してこれが可能になります。最初に 2 つの暗号鍵が作成され、どちらかを公開鍵として使用できます。つまり、2 つのうちどちらの鍵を使っても、一方の鍵が復号化に使われるなら、他方の鍵を暗号化に使用できます (復号化に使う鍵を秘密にしておきます) 。

一方の暗号鍵を公開鍵、もう一方の暗号鍵を秘密鍵として使うことに決めた後でも、秘密鍵でメッセージを暗号化することは可能です。しかしこの場合、あなたの公開鍵を持っていれば誰もがメッセージを解読できます。公開鍵はその名のとおり公開してあるので誰でも(あなたの秘密鍵で暗号化された)メッセージを解読できてしまい、この暗号化ではメッセージのプライバシーをまったく守れません。

ところで、あなたの公開鍵で解読できたメッセージを暗号化しうる唯一の人物は、あなた、つまり、秘密鍵を持っているあなただけだ、ということにお気づきでしょう。メッセージを秘密鍵で暗号化することは、デジタル署名に相当し、暗号化署名 cryptographic signing と呼ばれます。実際、暗号署名は、真正性に関する 2 つの特性を実現できます。

1. 帰属性 Attribution。メッセージを書いたのは (他の人ではなく) あなたであること。

2. 完全性 Integrity。メッセージが書かれた通りに受け取られること、つまり改ざんされていないこと。

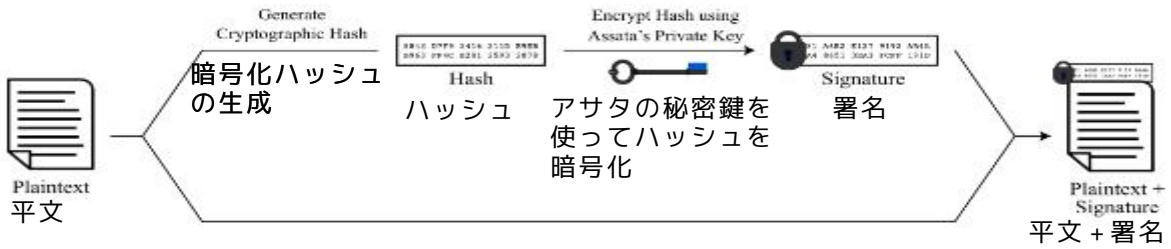
2 つ目の特性は、改ざん者が目的を達するためには、あなたの公開鍵で復号したときに改ざん者望むような平文が生成されるように暗号文を改ざんする必要がある、という事実に基くものです。しかし、これは全く実現不可能なのです。

これらの特性は、あなただけが自分の秘密鍵を管理しているという場合にのみ意味を持ちます。なぜなら、誰か他の人があなたの秘密鍵をもっていればテキストを変更して暗号署名することができてしまうからです。

暗号化ハッシュへのデジタル署名

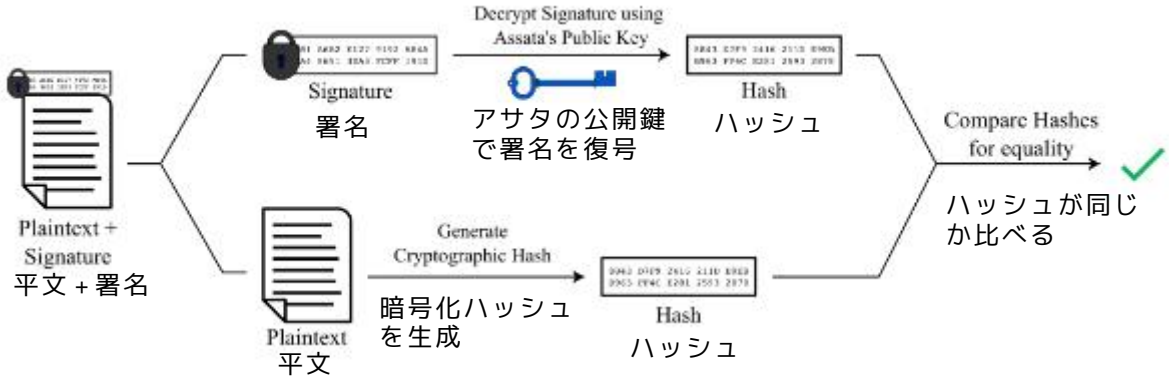
実際には、メッセージ全体を暗号化するのではなく、メッセージの暗号化ハッシュ (ダイジェストまたはフィンガープリント) を暗号化して、デジタル署名を行います。これは、効率性のためです。ここでは、アサタがメッセージに署名し、ボビーがその署名を検証するプロトコルを考えてみましょう (下図参照)。

アサタは、自分のメッセージの暗号化ハッシュを計算し、その結果を自分の秘密鍵で暗号化することでデジタル署名を作成し、メッセージに添付します。



署名の作成

ボビーはこの署名を受け取り、アサタの公開鍵を使って復号化すると、アサタが生成したものと同じ暗号化ハッシュが得られます。次に、ボビーは受け取っているメッセージの暗号化ハッシュを作成し、その結果をアサタから受け取って復号化された暗号化ハッシュと比較します。



暗号化ハッシュを偽造することは不可能である

暗号化ハッシュは偽造できないことを思い出してください。もし、ボビーが生成した 2 つのハッシュ（アサタのメッセージから直接生成したものと、アサタの署名から復号して生成したもの）が同じであれば、次の 2 つのことがわかります。

1．アサタだけが署名を生成できた。秘密鍵を持っているのはアサタだけなので、アサタの公開鍵で復号できるものを暗号化できる。

2．アサタがメッセージを書いてから、そのメッセージは変更されていない。もし誰かがメッセージを変更した場合、メッセージの暗号化ハッシュは、署名に含まれる暗号化ハッシュとは異なるはずです。それでは偽造がわかってしまうため偽造者は新しい署名を作成しなければなりませんが、アサタの秘密鍵がなければ署名を作成することはできません。

つまり、真正性を暗号技術で確認できたのです。

なお、エドガーは、中間者攻撃によって、単に署名を削除することができます。つまり、暗号化された署名を効果的に使うためには、暗号化署名をいつでも使うことに決めておく必要があります。[25]最近のエンド・ツー・エンドの暗号化メッセージングアプリには、一般的にデフォルトで署名が組み込まれていますが、これは一般のユーザーからはわからないことが多いのです。

暗号化された署名の用途

上記の例のように、暗号化された署名は、伝統的な手書きの署名や蝋印と同様に、メッセージに信頼性を与えることができます。しかし、デジタル署名が可能なのは、電子メールなどのメッセージには限りません。

ソフトウェアの検証

25 （訳注）常に署名があるのに、もし署名がなければ、そのこと自体が「異例」なことであり、メッージに何か問題があることを示唆することになる。

あまり意識されないかもしれませんが、デジタル署名の最も明確で一般的な利用方法は、ソフトウェアの検証でしょう。アプリなどのソフトウェアは、開発者からあなたのコンピュータや携帯電話に届くまでの間に誰かが手が加えなければ、開発者が望んだ通りの動作をします。責任ある開発者は、メッセージへの署名と同じように、製品に署名します。プログラムやアプリは、実際には単なるコンピュータファイル（または一連のファイル）であり、単なる文字の羅列でメッセージの一種にすぎません。開発者が公開鍵暗号方式でソフトウェアに署名している場合、注意深いユーザーは、開発者の公開鍵を入手して上記のような検証を行うことで、署名を確認することができます。(開発者は、あなたがソフトウェアをダウンロードした経路とは別の経路で公開鍵を提供しているはずです。これにより、「中間者」の章で説明したように、帯域外比較が可能になります。帯域外とは、検証に使用する公開鍵を、メッセージやソフトウェアのダウンロードとは違う通信経路（帯域）で取得したことに基づいています。）

フィンガープリント認証と「信頼の輪」の管理

アサタの公開鍵を信頼するために、ボビーはこれまで説明してきたように、鍵のフィンガープリントを確認することで、本当に彼女の公開鍵かどうかを検証しなければなりません。そうしないと、侵入者であるエドガーが自分の秘密鍵に対応する公開鍵をボビーに渡してしまう可能性があるからです。しかし、アサタの公開鍵が本当に彼女のものであることをボビーが確認した場合、ボビーはアサタの公開鍵に（自分の秘密鍵で）デジタル署名することができます。こうしておけば、ボビーは自分がすでに検証した公開鍵を確実に管理することができ、以下のようにすればアサタの公開鍵を他の人に知らせることができるのです。

クリーヴァーがアサタに暗号化メッセージを送信しようとしいて、エドガーが中間者を演じていないことを確認したいとします。しかし、クリーヴァーにはアサタの公開鍵を検証できるような別の通信経路がありません。ところがうまい具合にクリーヴァーはボビーの公開鍵を受け取ってそれを検証できています。そうなると、ボビーは自分の署名とともにアサタの公開鍵をクリーヴァーに送ることができます。クリーヴァーがボビーを信用し、ボビーの公開鍵を検証しているので、クリーヴァーはアサタの公開鍵についてのボビーのデジタル署名を検証し、アサタの公開鍵が本物であることを確信することができます。

これが「信頼の輪」の基本です。鍵のフィンガープリントが直接検証されていなくても、自分と目的の通信相手との間に信頼の道筋があれば、それを通して間接的に検証することができるのです。

コンテクスト：令状のカナリア

令状のカナリア Warrant canaries(またはカナリア声明)とは、公開された日付までにプロバイダが、データ漏洩、暗号鍵の開示、システムへのバックドアの提供など、ユーザを危険にさらす可能性のある手続き(合法・触法をとわず)の対象となっていなかったことをユーザに通知するものです。公表されたスケジュールどおりに声明が更新されない場合、ユーザーは、過去または将来のデータを危険にさらす可能性のある問題が発生したと推測することができます。例えば、Riseup.net では、四半期ごとにカナリア声明を発行しています。この声明には暗号化された署名が付されており、その真正性、つまり、このステートメントを書いたのが Riseup.net の人間であることを確認することができます。ま

た、公表日当日のニュース記事へのリンクを声明に掲載することで、声明がその日付以前に発表されたものではないことを証明しています。

米国では、米国政府が誰かに言論を差し控えることを強要する法的手続きがあり、それを回避するための手段として令状のカナリアが使われるようになりました。一方、米国政府は誰かに何かを、特に真実ではないことを語らせることはできないので、ユーザを危険に晒すような出来事は何もなかったとする偽のカナリア声明をプロバイダに強要することはできませんでした。

この言葉は、もともと炭鉱で毒ガスを検知するためにカナリアが使われていたことに由来するものです。

次に学ぶこと

メタデータ

外部リソース

Riseup. “Canary Statement” (英語) Accessed February 9, 2021.

Torプロジェクト. “How Can I Verify Tor Browser’s Signature?” (英語) Accessed February 9, 2021.

図版の出典

署名の作成 pgpsigning1 © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

暗号化ハッシュの偽造は不可能 pgpsigning2 © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

メタデータ

この章で学ぶこと

1. メタデータとは何か
2. メタデータでわかってしまうこと
3. メタデータの保護が難しい理由

メタデータとは何か？

メタデータとは、データそのものではなく、データに付随するあらゆる情報のことす。いくつかの例を挙げて説明します。

1．電話の場合、メタデータには、自分や相手の電話番号、通話の開始時刻、通話時間などがあります。携帯電話の場合、メタデータには携帯電話の位置（GPS 座標）、接続されている基地局、さらには使用している携帯電話の機種などが含まれるでしょう。電話のメタデータには伝送される音声そのものは含まれず、音声は「データ」です。電話のメタデータは、かつては通話料金の請求書作成のために必要とされました。

2．最近のデジタル写真には、撮影した時間や場所、使用したカメラの種類や設定などの情報が含まれていることが多くみられます。この場合、写真そのものがデータとなります。Facebook、Twitter、Instagram などの多くのウェブサイトでは、あなたが写真やビデオをアップロードする際に、プライバシー保護のためにこのメタデータを削除しています。また、Google、Flickr、YouTube など、そうした措置をとっていないサイトもあります。

3．最近のほぼすべてのカラープリンターは、米国政府が貨幣の偽造に使用される恐れがあるとしてプリンターメーカーに要請した結果、フォレンジックコードを各ページに印刷するようになっています。フォレンジックコードは目で見えるものも見えないものもあります。この場合、ユーザーが意図して印刷した情報（フォレンジックコードを除いたもの）がデータ、フォレンジックコードによってエンコードされた情報がメタデータとなります。フォレンジックコードには、印刷日時、プリンターのシリアル番号などが含まれます。

エドワード・スノーデンが最初に公開した情報で、NSA はベライゾンの顧客がかけた電話のメタデータをすべて収集していたことが明らかになり、メタデータに関する議論が世間に広まりました。これをきっかけにしてどのようにプライバシーが侵害されているのか、という議論が続いたのです。この年の初め、AP 通信社は、司法省からメタデータの提出命令を受けていましたが、AP は「これらの記録は、2 ヶ月間に AP 通信社が行ったすべてのニュース収集活動における機密情報源とのコミュニケーションが明らかにされる可能性があり、AP 通信社のニュース収集活動拠点も漏洩し、AP 通信社の活動と運営に関する情報を開示するものであるが、それら関して政府には知る権利がない」との理由で命令を無効にするように訴えました。裁判所の判決理由では、このようにメタデータを使って集めた GPS データから「毎週教会に通っているのか、大酒飲みなのか、ジムの常連なのか、浮気をしている夫なのか、治療を受けている外来患者なのか、特定の個人や政治団体の仲間なのかを推測することができる 」と指摘しています。

NSA は内部文書の中で、メタデータを同機関の 「最も有用なツール」の一つとしています。

メタデータとインターネット

あなたがウェブサイトにアクセスすると、あなたのコンピュータとウェブサイトのあるサーバーとの間で、インターネットを通じて情報が送受されます。基本的には、あなたのコンピュータからサーバーに向けてウェブサイトのコンテンツを要求するメッセージが送信され、その後、サーバーからあなたのコンピュータにウェブサイトのコンテンツが返信されます。インターネット上で送信される情報は、しばしばトラフィックと呼ばれ、どこ

へ向かうにせよ伝達されるメッセージは、実際にはたくさんの短いパケットに分割されています。各パケットには主要部分が 3 つあります。

1. ヘッダーには、送信者と受信者（あなたのコンピューターとウェブサイトのサーバーなど）それぞれのインターネットアドレスと、送信されるデータの種類（HTML など）が記載されています。

2. データとは、メッセージの内容（例えば、そのウェブページ内容の全体や一部）のことです。

3. トレーラーは、パケットの終わりを明示し、パケットが転送中に破損していないことを確認するものです（ハッシュ関数を使用）。

このようなパケットではヘッダとトレーラがメタデータです。ヘッダーは、パケットの送信先を示すものであるため、保護や隠蔽が難しいものです。手紙を送るのと同じように、配達には住所が必要です。インターネット上の住所（IP アドレス）は、あなたの物理的な位置に関連しており、実際、IP アドレスからあなたの物理的な位置が特定できることがよくあります。

この説明は、電子メール、ビデオストリーミング、VOIP 通話、インスタントメッセージなど、インターネット上で送信されるあらゆる情報に当てはまります。

コンテクスト： 内部告発者の保護

2017 年 5 月、リアリティ・ウィナー Reality Winner は、2016 年の米国大統領選挙へのロシアの干渉について報告した NSA の文書を公開しました。この記事が公開される数日前に彼女が逮捕されたことで、なぜ彼女がすぐに内部告発者として特定されたのかについて多くの憶測を呼び、多くの人がこの記事の取り扱いについてウェブサイト「Intercept」の責任を指摘しました。リアリティ・ウィナーは、匿名で文書のカラープリントをインターセプトに郵送しました。インターセプトは通常のジャーナリズムのルールに則り、検証のために文書の写真を NSA に送り、同じ写真を再編集して報道しました。この記事が公開された直後、何人かの人が、写真の中にプリンタのフォレンジックコードが見え、文書が印刷された日時とプリンタのシリアル番号が判別できたと指摘しました。この情報から FBI がリアリティ・ウィナーを特定できた可能性もありますが（情報源を保護するために、Intercept は写真のフォレンジックコードを編集すべきでした）、彼女の仕事用コンピュータのファイルアクセスのログから身元が判明した可能性の方が高いと思われます。

次に学ぶこと

匿名ルーティング

外部リソース

CNN. “AP Blasts Feds for Phone Records Search.” May 14, 2013.

電子フロンティア財団. “Justice Department Subpoena of AP Journalists Shows Need to Protecting Calling Records.”. May 13, 2013.

電子フロンティア財団. “Secret Code in Color Printers Lets Government Track You.” October 16, 2005.

Snowden Archive-the SIDtoday Files. “The Rewards of Metadata.” Intercept, January 23, 2004.

New Yorker. “The Metadata Program in Eleven Documents”. 2013 年 12 月 31 日

Intercept. “Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election.” June 5, 2017.

Atlantic. “The Mysterious Printer Code That Could Have Led the FBI to Reality Winner.” June 6, 2017.

匿名ルーティング

この章を読む前に、「暗号化のための鍵の交換」と「メタデータ」の章を読むことをお勧めします。

この章で学ぶこと

1. インターネットでは誰が何にアクセスできるのか
2. オンラインでの匿名コミュニケーションを可能にする技術
3. 匿名性とは何か、匿名性の落とし穴はどこにあるのか

オンライン通信ではインスタントメッセージや電子メール、ウェブの閲覧など、さまざまな情報がコンピュータに送られてきます。この章では、主にウェブ閲覧について説明しますが、それ以外のほとんどの場面でも同じ考え方が適用できます。コンピュータのアドレス（IP アドレス）は、インターネット通信で情報パケットがコンピュータに到達するための手段であり、住所があれば封筒や荷物が郵便受けに届くのと同じです。そのため、コンピュータの現在の IP アドレス（インターネットに接続している場所によって変わります）は、あなたの物理的な位置に関連しています。その物理的な場所がどれほど精密にわかるかは、インターネット・サービス・プロバイダ（ISP）がどれだけの情報を公開し、誰に対して公開するのかによって決まります。ISP は、あなたがどのケーブルテレビ回線、どの電話回線、またはどの携帯基地を通じてインターネットに接続しているのかを知っていますが、IP 位置情報（ジオロケーション）検索サイトに郵便番号程度の情報を提供するだけかもしれません。あるいは家の位置情報までも提供する場合があります。

IP アドレスは、あなたのコンピュータに情報を送るために必要なメタデータの 1 つに過ぎません。しかしウェブを閲覧する際には、厳密に言えば必要のない他のメタデータがたくさん、「あなたの閲覧体験を最大限に高める」ために送信されます。このような情報の例としては、使用中のブラウザに組み込んだプラグインの名前、タイムゾーン(日本時間、

など）、コンピュータの画面サイズといった詳細があります。これらはあなたがインターネットに接続する際に使用する IP アドレスが変わった場合でもあなたを特定するための識別子となるのです。

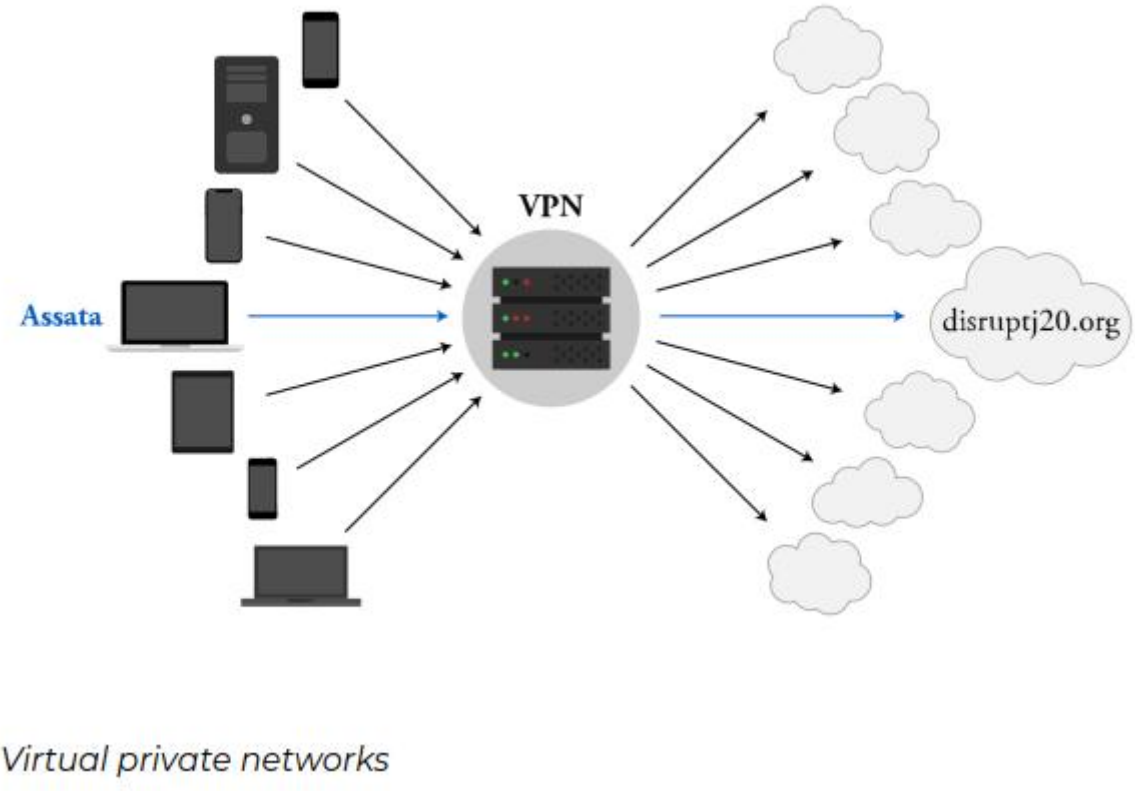
では、このような個人を特定できるメタデータにアクセスできるのは誰なのでしょうか。もし https のような暗号化がなければ、盗聴者はメタデータだけでなく、通信内容にもアクセスできてしまいます。暗号化されていればメタデータの一部は ISP や盗聴者から保護されますが（どのブラウザを使用しているかなど）、IP アドレスやアクセスしているウェブサイトのドメイン情報は保護されません。また、閲覧しているウェブサイトのサーバーは、コンテンツだけでなく、メタデータにもアクセスできます。

ところで、あなたに情報を提供するために使用されるメタデータを保護する方法はないのでしょうか、また、誰から保護することができるのでしょうか。ここでは、ウェブ閲覧を匿名化する 2 つの方法について説明します。

中間者を信じて使う：仮想プライベート・ネットワーク

仮想プライベート・ネットワーク（VPN）技術は、大学や会社内のネットワークなどのローカル・ネットワークを、キャンパス外の住宅やホーム・オフィスなどのリモート地点にも拡張し、大学や会社の外にいても、ローカル・ネットワークにいるときと同じ資源（図書館の学内サービスやソフトウェアの社内契約など）を使えるようにするための手段として始まりました。VPN に接続している間、ウエッブページのホストは、ローカルネットワークの IP アドレスを、VPN によって拡張されているあなたのアドレス、つまりあなたの自宅の IP アドレスであるかのように認識します。このような理由から、VPN は位置情報を匿名化するために使用されています。

VPN は、無害であることが期待される中間者として動作します（下図参照）。アサタは、ウェブサーバーへのリクエストを直接送信するのではなく、リクエストはすべてを VPN に送信します。また VPN はインターネットからリクエストの応答を取得し、それをアサタに送信します。この方法の詳細は、VPN サービスによって異なりますが、一般的に、あなたと VPN の間の通信は暗号化されます。VPN の保護品質は、その VPN にどれほど多くの人々が接続しているかにも依存しています。VPN との通信を監視している盗聴者は、VPN に接続している個人と、VPN とウェブサーバー間で通信されるリクエストとを特定することができますが、VPN に出入りするリクエストが大量になれば、リクエストと対応するユーザーとを完全には照合することができません。



仮想プライベート・ネットワーク(VPN)[26]

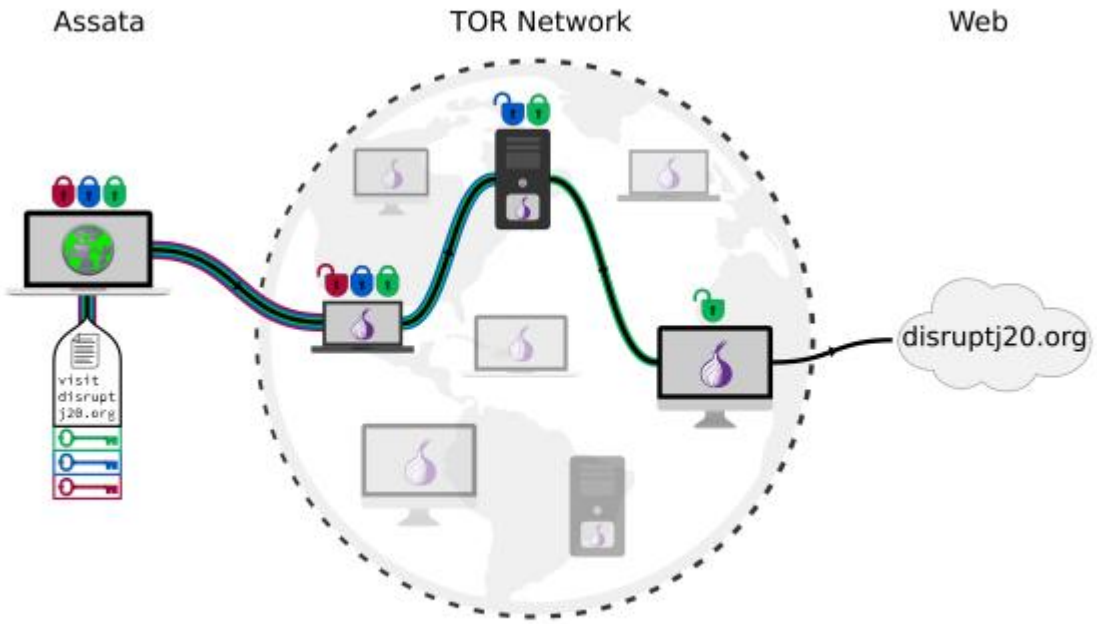
もちろん、VPN プロバイダはあなたのインターネット上での行動をすべて把握していますし、VPN プロバイダの協力があれば敵も同様に把握することができます。つまり、あなたは自分の情報の保護についてその VPN プロバイダーを信頼いるということになります。しかし、VPN の使用とは無関係に ISP も、同じ情報にアクセスすることができます。あなたは、ISP を信頼するのと同じように、VPN プロバイダーを信頼しているのです。違いは、あなたの ISP はインターネット上の宛先サーバーに対してあなたの IP アドレスを隠蔽しないのに対し、VPN は隠蔽するということです。しかし、同じ VPN を多くの接続場所（自宅、職場、喫茶店など）から使用すると、当の VPN という単一の組織に各接続場所のインターネット利用状況を完全に把握されてしまうため、ISP よりもプライバシーリスクが多少高くなります。

中間者を信用しなくてよい：Onion Router（オニオン・ルーター）

Onion Router（Tor）は、信頼性の問題を回避しながら匿名でインターネットにアクセスするための手段であり、その名前は暗号化の層（玉ねぎの層のような）を使用することに由来しています。すべての情報を信頼できる 1 つの仲介者を通すのではなく、何千ものボランティアサーバーからランダムに選ばれた（少なくとも）3 つの仲介者を使います（下図）。この仲介者の経路を通るトラフィックは暗号化されていて、最初の（入口）ノードはあなたが Tor 経由でインターネットにアクセスしていることだけを知り、2 番目の（中

26 (訳注)この図で用いられている http://www.disruptj20.org は実在のサイト。2017 年 1 月のトランプ大統領就任を阻止するワシントン DC の草の根運動のサイト。現在もアクセス可能。本章の最後に紹介がある。

継）ノードは誰かが Tor 経由でインターネット上の何かにアクセスしていることだけを知り（ただし、具体的に誰が、具体的に何に、ということではなく）、最後の（出口）ノードはある（例えば）ウェブページが Tor ユーザーによってリクエストされていることだけを知るのです（ただし、リクエストしたのがどの Tor ユーザーかはわからない）。



Tor

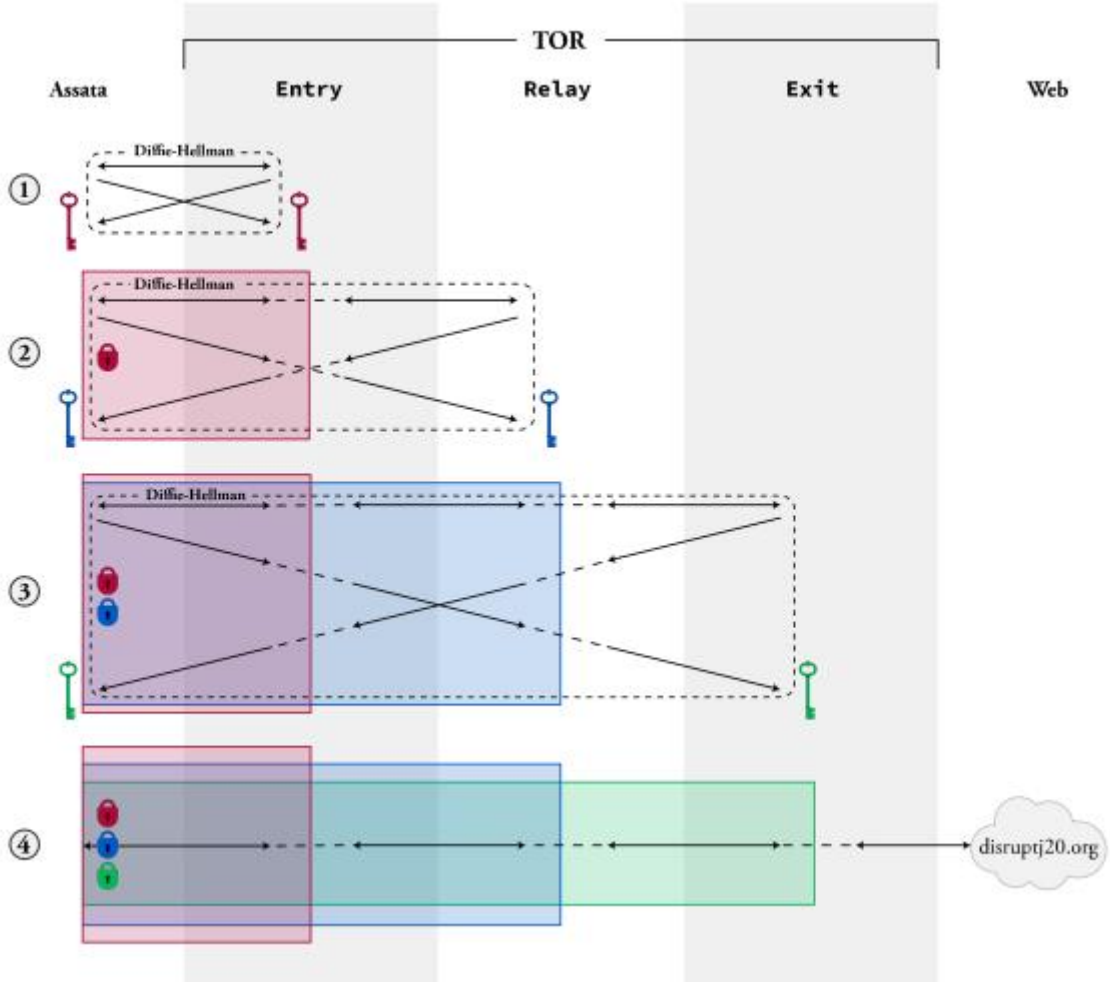
この方法は、以下のようなデフィー・ヘルマン鍵交換によって行われます（下の図を参照）。

(1) アサタは、入口ノードと共有している暗号鍵（赤で示したものを入口鍵と呼ぶ）を設定する。これにより、アサタと入口ノードの間に暗号化された通信チャネルが確立される。

(2) アサタはこの暗号化通信路を使って、入口ノードを介して中継ノードと通信する。入口ノードと中継ノードの間の通信は暗号化されていないが、入口ノード経由のチャネルを使って、アサタは中継ノードと共有する暗号鍵（青字の中継鍵）を確立する。中継ノードが知っているのは、ある Tor ユーザーと共有鍵を設定していることだけで、その Tor ユーザーの身元は知りえない。

(3)このプロセスをもう一度繰り返して、アサタは出口ノードと共有する暗号化キーを確立する（緑の部分が出口キー）。

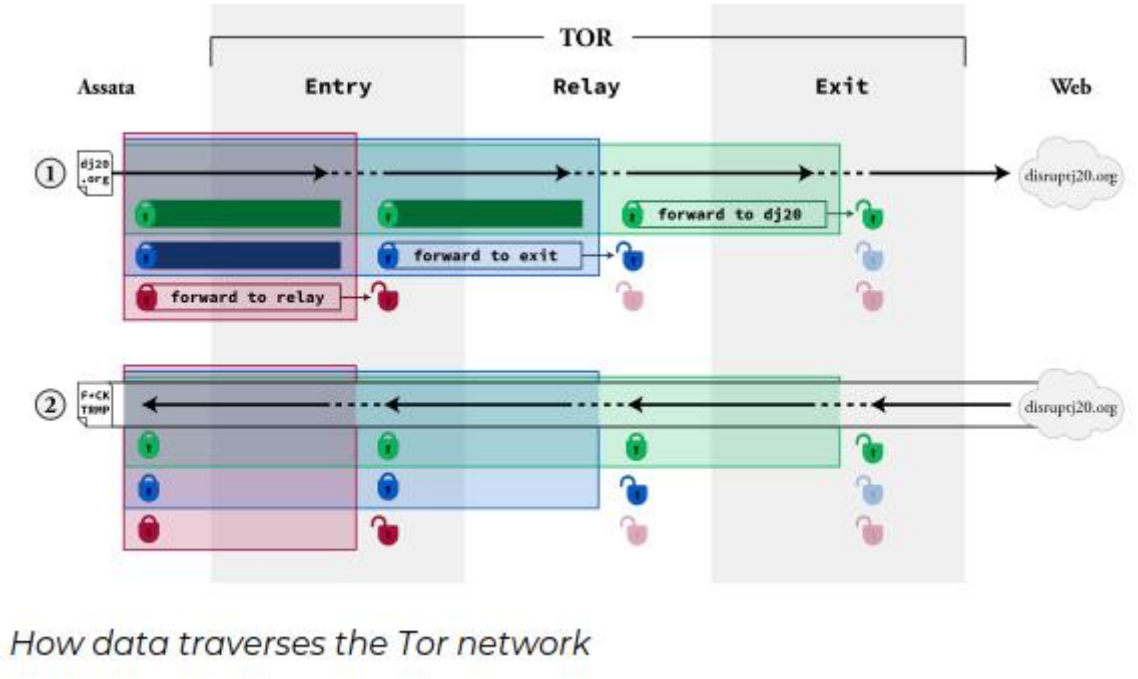
(4) ここまでのプロセスにより、アサタと入口ノード、中継ノード、出口ノードとの間でそれぞれ暗号化を行うための一連の鍵（赤、青、緑）が作成されました。



Tor が Diffie-Hellman 鍵交換を使って鍵を確立する方法

アサタが disruptj20.org にリクエストを送る場合、彼女は disruptj20.org 宛てのリクエストを緑の鍵で暗号化してを出口ノードに送るのですが、これはさらに次のようにして暗号化されるのです。「緑暗号化」されているリクエストを中継ノード宛てのメッセージに組み立てて青の鍵で暗号化し、さらにこれを入口ノード宛てのメッセージに組み立てて赤の鍵で暗号化します。アサタがこの「赤暗号化」メッセージを赤の入口ノードに送信すると、入口ノードでは（アサタと共有している赤の鍵で）第 1 層の暗号を復号して、中継ノード宛てのメッセージが得られます。これを受け取った中継ノードで第 2 層の暗号を復号すると（このときは中継ノードがアサタと共有している青色の鍵を使用）、出口ノード宛てのメッセージが得られます。これを受け取った出口ノードが暗号を解くと（出口ノードがアサタと共有している緑色の鍵を使います）、disruptj20.org 宛てのメッセージが得られ、出口ノードはこのリクエストを転送します。これが下の図の①です。

disruptj20.org がアサタのリクエストに返信するとき、ウェブサーバは情報を出口ノードに送り返します。出口ノードは緑の鍵で暗号化し、それを中継ノードに送ります。中継ノードは青の鍵で暗号化し、それを入口ノードに送ります。入口ノードは赤の鍵で暗号化し、それをアサタに送ります。アサタは、必要な鍵をすべて持っているので、3 つの暗号化層をすべて復号することができます。これは下の図で②の部分です。



データが Tor ネットワークを通過する仕組み

あなたの情報が Tor ネットワークを通過したときの経路を再現し、その結果あなたのウェブリクエストを見つけ出すためには、敵対者はあなたが入口・中継・出口として選択した 3 つのノードをすべて監視しなければなりません。敵がたとえ Tor ネットワークの 80%を支配していても、あなたが選択した 3 つのノードすべてを支配できる可能性は 50%しかありません。Tor のノードは何千もあり、誰でもボランティアで操作することができるので、これはあり得ないことといっていいでしょう。

これとは別の攻撃手段として、確認攻撃 confirmation attack があります。このシナリオでは、敵対者はあなたが特定のウェブサービスを訪れたことを証明しようとします。もし敵対者が、（例えば ISP を通過している）あなたのウェブ・トラフィックと対象ウェブ・サービスのウェブ・トラフィックに（合法的あるいは法外な手段で）アクセスできれば、敵対者は、あなたが Tor を使用したタイミングと Tor からウェブ・サービスにアクセスしたタイミングに基づいて、照合できるかもしれません。このような関係検出手段は、活動家集団「Anonymous」が行ったハッキング活動で有罪判決を受けた Jeremy Hammond 事件でも使用されました。

他にも Tor への攻撃は行われていますが、Tor プロジェクトはその技術やセキュリティをとても積極的に改善しています。匿名ブラウジングへの妨害についてすぐ後に説明します。また、ユーザーが陥る可能性のある落とし穴や、匿名でウェブにアクセスしようとする際のベストプラクティスについては、後の方の「自分のアイデンティティを守る」の章で説明します。

匿名ブラウジング技術の利用とそれへの妨害

中国やイランなど、インターネットがいつも検閲されている国では、多くの人が VPN や Tor を利用して検閲を回避しながらウェブにアクセスしています。一方で、インターネッ

ト通信のメタデータから VPN トラフィックの証拠を得ることができるため、政府はこれを利用して、中国やシリアでの検閲のように、そのような通信をすべてブロックすることもできます。また、イランのように、政府が認可していない特定の VPN プロバイダーへのアクセスを遮断する国もあります。

Tor のノードは公開されているので、政府などは Tor アクセスを一切使用できないようにすることができます。これは単純に Tor ノード宛の通信を全て遮断することで可能です。これを克服するには、ブリッジを使用します。ブリッジとは一群の非公開 Tor ノードで、公開された入口ノードの代わりになるものです。ブリッジノードは少数しか運用されていないので、そこへアクセスするには、特定のメールアカウント（例：Google、Riseup!、Yahoo!）から Tor プロジェクトにメールを送ってリクエストする必要があります。Tor での通信は VPN トラフィックの場合と同様に、パケットインスペクション[27]、つまり通信のメタデータを調べることでもブロックされてしまいます。Tor プロジェクトでは、インターネット上の Tor トラフィックを難読化して Tor のトラフィックであると見られないようにする方法を用いて、このような妨害を困難にしています。

また、VPN や Tor は、ウェブホストが意図的に特定の地域からは利用できなくしているサイトにアクセスするためにも使用されます。これは、Hulu や Netflix などのメディアプラットフォームではよく見られます。そのため、コンテンツ企業が既知の VPN サービス・プロバイダーや Tor の出口ノードからのアクセスをブロックすることも、しばしば行われます。

コンテクスト： Ðisruptj20

2017 年 1 月 20 日、米国第 45 代大統領の就任式の前後には大規模な抗議活動が行われました。これらのイベント実行の多くは、disruptj20.org というウェブサイトでコーディネートされていました。2017 年 8 月には米国司法省が disruptj20.org のウェブホストである ÐreamHost に対して、「すべての HTTP リクエストおよびエラーログ」を要求する令状を発行したことが明らかになりました。このログには、ウェブサイトを訪れた 130 万人とも言われるすべての個人の IP アドレス、どのウェブページを訪れたか、その頻度、訪問者がウェブページに入力したテキストなどが含まれています。

もちろん、匿名ブラウジング技術を使っていたサイト訪問者の IP アドレスは保護されたことでしょう。

次に学ぶこと

自分のアイデンティティを守るために

外部リソース

27 （訳注）インスペクションは「何らかの対象を精査したり監視・追跡すること」。パケットインスペクションは、「ネットワークの境界などに設置されたルータなどの装置が、内外を流通するデータ（パケット）を監視すること」(https://e-words.jp/)

Great Firewall of China では、中国でどのサイトが何回、どのように検閲されたかを記録しています。

Search Warrant to ÐreamHost（2017年8月）

図版の出典

仮想プライベート・ネットワーク(VPN)anonymous-browsing-vpn © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

Tor anonymous-browsing-tor © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

Tor が Ðiffie-Hellman 鍵交換を使って鍵を確立する方法 anonymous-browsing-TOR-1-keyexchange © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

データが Tor ネットワークを通過する仕組み anonymous-browsing-TOR-2-data-transfer © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

Part2：社会運動へのデジタルな抑圧 社会運動へのデジタルな抑圧（アメリカ編）

社会運動抑圧のメカニズム

本章を読む前に、序章の「なぜデジタル・セキュリティなのか」をお読みください。ここでは米国の社会運動に焦点を当てていることに注意してください。

この章で学ぶこと

1．米国政府はどのようにして社会運動を抑圧しているのか

2．コインテルプロ（対敵諜報プログラム）とは何だったのか、そして当時の社会運動を抑圧するために用いられたメカニズムはどのようなものだったのか

米国には、自国を含めて社会運動、特にリベラルや左翼的な社会運動を抑圧するという形で干渉してきた長い歴史があります。労働者の組織化、独立運動、公民権運動、環境保護運動などが、しばしば大企業の要請や協力を受けた米国政府の敵視政策に遭ってきました。

社会運動がデジタル・セキュリティに無頓着だったらどのようなリスクがあるのでしょうか。ここでは過去に国家がどのように社会運動を妨害してきたかを見ると役に立ちます。このような歴史を知ると、ときには圧倒され、過去に起こったことで今は起こっていないと片付けたくなることもあります。あるいはこのような歴史を振り返ることで敗北主義につながる恐れさえあります。特に敵対者とみなされたり、国家が実際に敵対している人々に対して使用できるデジタル的に強化されたツールが増えていることを考えるとなおさらです。

しかし、過去の過ちを繰り返すべきではないので、十分に歴史を学び、適切な教訓を得て、私たちの運動が今後も成功するようにしなければなりません。歴史の教科書に敗北の事例を増やさないために、20世紀に米国政府が社会運動を混乱させた方法を分類したジュールズ・ボイコフ Jules Boykoff の研究を参考にします。ボイコフは抑圧の手口として12種類を列挙していますが、ここでは7種類に絞ります。

これらの歴史的なありさまを理解することで、「社会運動へのデジタルな抑圧」の章で説明するように、現代のデジタル監視がこれらの抑圧をどのように支え、強化していくかを予測することができます。しかし、より重要なのは、本書の第3部で取り上げるように、暗号化やデジタル予防策に気を配ることで、これらの抑圧勢力（の少なくとも一部）から社会運動をどのように守れるかを知ることができるのです。

抑圧の手口

米国政府が社会運動を抑圧してきた、そして今も抑圧し続けている7つの方法を、それぞれの使用例を交えて紹介します。残念ながら、これらの例だけですべてを網羅できるわけではありません。

1．直接的な暴力

殴打、爆破、銃撃、その他の形態の暴力が、国家やその他の機関、権力側組織によって反体制市民に対して行われます。

このような直接暴力には、大きな集団に対する制圧（オハイオ州兵の警備隊がケント州立大学での反戦抗議活動中の学生に発砲し、4人が死亡、9人が負傷した事件など）や、標的を絞った暗殺（FBIが計画した夜襲でブラックパンサー党のリーダー、フレッド・ハンプトンが射殺された事件など）の例があります。控えめに言っても、これらの行為は、生命や身体への恐れを生じさせ、社会運動への参加を妨害するものです。

2．法制度

嫌がらせ目的の逮捕、訴追、尋問、あるいは特別な法律を使って偏見のあるやり口で個人に干渉する、といった法制度が存在します。国家は、しばしば虚偽の微罪で活動家を逮捕したり、長い間適用されたこともないあいまいな法律を根拠にしたして活動家を逮捕したりしており、差別的な法的迫害の枠組を悪用しています。訴追や尋問によって、反体制派の人々は刑務所に入れられたり、法的手続きに労力を費やされたりして、活動が妨げられ、運動を停滞させられてしまいます。支持者や潜在的な仲間となりうる人たちが、反体制的な意見を述べることを躊躇するように仕向けているのです。マスメディアで訴追や尋問が公表されると、一般の人々にまで波及します。もうひとつの法的抑圧は、国家が例外的な法律や規則を公布・施行して、活動家を刑事司法の迷宮に縛り付けることです。このようにして、反対意見を封じ込めるために法制度が使われています。

物議を醸している「ストップ＆フリスク」[28]プログラムは、警察官が正当な理由なしに人々を短時間にせよ拘束し、時には捜索することを可能にしています。“言論の自由の範囲”を狭く設定すれば、抗議活動の時間、場所、方法が大幅に制限されます。ドナルド・トランプ大統領の就任式の際、米国憲法修正第1条で保護されている抗議活動を行ったことで逮捕された人々は、ほとんど有罪判決の可能性がないのに起訴されました。また、放火や器物損壊などの特定類型の犯罪は、政治的な動機を伴うと“テロリズム“に格上げされ、国が科す罰を大幅に重罰化させることができます。他にも、（動物虐待を暴露するために行われる）飼育現場の撮影を犯罪とする「ag-gag法」[29]など、社会運動のための活動を阻止するためにわざわざ作られた法律もあります。

3.雇用の剥奪

政治的信念や活動が原因で、雇用を脅かされたり、実際に失ったりすることがあります。反体制派の中には、政治的信条を理由に、そもそも雇用に至らない人もいます。雇用の妨害は一般的には雇用主が行うものですが、国が直接・間接的に強力な影響力を持つこともあります。

最近では、大学教授が職を追われたり、採用が取り消されたりするケースも見られます。スティーブン・サライタ Steven Salaitaはイスラエルやシオニズムを批判する一連のツイートを行ったために、大学の寄付者が反対を表明してアメリカ・インディアン研究の教

28 （訳注） 警察官が路上で不審な人物を制止して行う職務質問および所持品検査
29 （訳注） 訳注：畜産分野での内部告発などを違法化する米国の法律

授への採用が取り消されました。テキサス州では政府・自治体の契約職員となるために、数年前から、パレスチナ人の BDS 運動[30]に参加しないという誓約書の署名を求められ、そうしなければ契約を取り消されることになっていました（連邦裁判所によってこの措置は取り消されました）。この制度のために、署名を断ったパレスチナ系米国人の言語療法士が解雇される事件がありました。

4.あからさまな監視

あからさまな監視をする目的は、情報収集ではなく、威嚇です。(情報収集なら秘密裏にするほうが効果的ですから。）これは、報復を恐れて言論を控えるという萎縮効果をもたらすことを目的としています。これにより、活動をしている人たちが離れていったり、新しい活動家を得ることが難しくなったりする可能性があります。このような萎縮効果をねらうことは米国で違憲とされていますが、裁判所で被害を証明することが難しいため、（監視する側からすれば）やりやすい弾圧手段といえます。

FBI は、反体制派や活動家の家（およびその家族や雇用者の家）を訪問して「ノック・アンド・トーク」や単純に「おしゃべり」をすることで近隣住民にこの家が警察に監視されていることを知らせるというやり方を長いことやってきた歴史があります。

5.秘密の監視

標的を絞った監視の手段には、スパイの侵入、特定対象の盗聴、データ提出命令や令状などが使われます。潜入者（対象グループのメンバーになりすました隠密エージェント）、情報提供者（グループのメンバーから金銭や脅迫で情報を引き出す）の利用などもあります。また、インターネットの監視や郵便の開封など、大量監視技術によって得られた個人や集団の情報を収集し、保存し、分析するなどによっても監視対象が広範に及ぶことがあります。

FBI の情報提供プログラムは大規模なもので、2008 年には 1 万 5 千人以上の情報提供者がいました。9.11 の後、FBI やニューヨーク市警などの大規模な法執行機関は、情報プログラムをイスラム系アメリカ人コミュニティに向けて展開しました。その中には、弁護士や教授、アメリカ最大のイスラム系市民権団体（アメリカ・イスラム関係評議会 the Council on American-Islamic Relations）の事務局長を FBI が監視するということも含まれていました。ニューヨーク市警は情報提供者や潜入者、監視技術を使って、モスクやイスラム教徒の学生団体、組織、企業などを狙って監視しました。潜在的な「テロリスト」を特定するためと称して市警は「過激化の兆候」に目を光らせたのですが、それは憲法修正第 1 条[31]

30（訳注)BDS 運動は、イスラエルが、①パレスチナ占領の終結、②イスラエルにおけるアパルトヘイト政策の中止、③パレスチナ難民の帰還権の承認という、3 つの国際法上の義務を履行するまで、同国に対するボイコット（Boycott）、資本引き揚げ（Ðivestment）、制裁（Sanctions）を市民・企業・政府に対して呼びかける国際運動。https://bdsjapan.wordpress.com/aboutus/

31（訳注)修正第 1 条［信教・言論・出版・集会の自由、請願権 ］［ 1791 年成立 ］
連邦議会は、国教を定めまたは自由な宗教活動を禁止する法律、言論または出版の自由を制限する法律、ならびに国民が平穏に集会する権利および苦痛の救済を求めて政府に請願する権利を制限する法律は、これを制定してはならない。（https://americancenterjapan.com/aboutusa/laws/2569/）

で保護されているような「イスラムの伝統的な服を着てひげを生やしている」「社会活動に参加する」といった活動が対象にされていました。

6. 騙し

“濡れ衣”*密告者ジャケッティング*Snitch jacketingとは、多くの場合潜入者の工作によって、本物の活動家を政府への密告者だとかグループに悪意を抱いているといった疑念を組織内部に植え付けることをいいます。単にグループの活動を当局へ報告するのではなく、グループに暴力や違法な活動・戦術を促す役割を持った潜入者は、かく乱工作員と呼ばれ、グループを法的危機に陥れたり、グループの信用を失墜させたりする活動を行います。“虚偽のプロパガンダ“とは、活動家の組織間に分裂を誘発させたり、連帯を損なったりする目的で文書をでっちあげることを意味します。このような、対立を作りだしたり、不快感を与えたり、時に悪質な文書で、グループ内やグループ間の不和を煽るのです

FBIの潜入者も撹乱工作を行い、違法行為を誘導したりします。FBIの潜入捜査官はオレゴン州立大学の学生だったモハメド・モハムドに接触し、2010年11月26日のポートランドのクリスマスツリー点灯式で爆弾を仕掛けるように5ヶ月間にわたって促し、資材も提供していました。爆弾は偽物でしたが、モハムドは懲役30年の判決を受けました。

FBIの別の情報提供者は、撹乱工作として、エリック・マクデイビッドのグループに企業や政府の施設破壊を唆すとともに、爆弾製造の情報、必要な原材料を購入するための資金、輸送手段、作業用の小屋を提供しました。マクデイビッドは、企業や政府の資産を破壊することを共謀した罪で約9年間の刑期を過ごしましたが、FBIが彼の無罪につながる証拠を弁護側に開示しなかったため、マクディビッドの有罪判決は取り消されました。

7.マスメディアの影響

マスメディアへの影響には、大きく分けて2種類あります。1）政府が作成した記事をそのまま、あるいは若干の修正を加えだだけで掲載する政府寄りの報道関係者を利用する「ストーリー・インプラント（記事注入）」と、（2）ジャーナリストや編集者を脅して不要な情報が掲載されないよう圧力をかける「ストロング・アーミング（力づく）」です。これらに加えて、マスメディアは反体制派を、非常識だ、尋常ではない、危険だなど、社会の主流から外れたものとして描かれます。これは陰謀によるよりも、ジャーナリズムの規範や価値観を映していることが多いのです。抗議活動やデモ行進などの際に、活動家と国が参加人数の見積もりに違いがでたときに、マスメディアが国の低い数字を受け入れ、運動を過小評価する傾向にもみられます。また、マスメディアは、反体制派の主張と体制派のそれを表面的にバランスさせることもあります。反体制派の活動の多くは、マスメディアの掲載方針に合わなかったり、新聞のベタ記事として埋もれてしまいます。こうして国家だけでなく、強力なメディア組織やメディアの個人オーナーもこのようにして弾圧を行うことができます。

9.11後のイラク侵攻の頃には、反戦感情が一貫して過小評価されてきました。例えば、2006年9月に全米で20万人以上が参加した反戦デモについて、オレゴニアン紙はワシントンDCで行われた10万人規模の反戦デモをポートランドで行われたデモの記事と一緒にして10面に掲載するという扱いをしました。ポートランドのデモ参加者は100人ほどだったと報じましたが、ヘリからの映像を見れば3000人以上だったことがわかります。

その一方でワシントン DC で行われた反戦デモへのカウンターデモには 400 人しか参加しなかったにもかかわらず、2 ページ目に大きな写真と長い文章で紹介したのです。

情報技術による妨害

検閲やその他の情報技術への干渉について語らなければ、ここでの議論は不十分でしょう。特に情報化時代に関連し、欺瞞やマスメディアの影響力とも結びついた抑圧が多発しています。例えば、抗議活動中にインターネットやモバイルネットワークへのアクセスを遮断したり、特定のサイトや特定の種類のインターネット通信だけを遮断したり、社会運動グループのウェブサイトを閉鎖したりすることなどです。

こういった手段はボイコフの“弾圧カタログ“には含まれていません。というのも、米国内では主に憲法で保護されているために、この方法が広まっていないのです。しかし、上述のようなやり口は世界中で広がっています。[32]政府は、国レベルでインターネットへのアクセスを遮断したり（抗議活動を抑制する手段として、イランで 1 週間にわたってインターネットを全面的に遮断した例など）、特定サイトへのアクセスを制限したりすることで知られています（中国のグレートファイアウォールが Google、 Facebook、 Twitter、 Wikipedia を遮断した例など）。米国の企業もこれに参加し、外国での検閲に「協力」しています。Zoom（ウェブ会議サービス）は、天安門事件のメモリアルとしてのオンラインイベントを計画していた 3 人の活動家のアカウントを、中国政府の要請に応じて停止しました。

コンテクスト **COINTELPRO** の時代

1950 年代から 1970 年代にかけて、FBI はエドガー・フーバー長官の指揮のもと、COINTELPRO（コインテル・プロ）[33]と呼ばれる一連の国内防諜活動を秘密裏に行っていました。“赤狩り“と呼ばれた米国政府の反共産主義プログラムに端を発したこの活動は、ブラックパワー、プエルトリコ独立運動、公民権運動などの組織化や活動を「必要であればあらゆる手段を講じて混乱させる」ことを目的としていました。公民権運動やブラックパワー運動（キング牧師の活動を含む）に関しては、黒人国家主義者やヘイトタイプの組織や団体、その指導者、スポークスマン、会員、支持者の活動を暴露し、混乱させ、誤った方向に導き、信用を失墜させ、その他の方法で無力化して、暴力や市民の混乱を引き起こす傾向に対抗する」ことが COINTELPRO の使命とされました。

COINTELPRO は、1971 年に発生した強盗事件で持ち出されていたたくさんの機密書類の箱が、当時活動中の FBI に対する市民調査委員会に渡ったことで発覚しました。ずっと後にエドワード・スノーデンの情報公開がきっかけになった情報公開法（Freedom of Information Act：FOIA）の請求によって、COINTELPRO のメンバーが公開され、他の COINTELPRO 文書も明らかになりました。先の FBI 調査委員会のリークにより、1975 年に米国上院のチャーチ委員会[34]が設立され、「個人のプライバシーを侵害し、合法的な集会

32 （訳注）たとえば、「世界各地のインターネット遮断のマッピング」（アルジャジーラ）、「#KeepItOn: 2021 年選挙ウォッチ」 参照。#KeepItOn は、政府などによるネット遮断に反対するグローバルなキャンペーン。

33 （訳注）**counterintelligence program**

34 （訳注）「CIA や FBI の権力乱用を捜査したチャーチ委員会」、デモクラシーナウジャパン

や政治的表現の権利を侵害した国内諜報活動」であるとしてFBIを非難し、最終的にCOINTELPROを停止させることになりました。チャーチ委員会報告はその前文で次のように警告しています。

> 私たちは、政府の一部が、その態度や行動において、民主主義にふさわしくなく、ときには全体主義体制を連想させる戦術を採用してきたことを目にしてきた。犯罪行為の防止や外国人スパイの特定といった限定的な目的で始められたプログラムが、証人が「掃除機」と表現したように、アメリカ市民の合法的な活動に関する情報を吸い込むまでに拡大されるという一貫したパターンを目の当たりにしてきた。情報活動が当初の範囲を超えて拡大していく傾向は、我々の調査結果のあらゆる側面に共通するテーマである。情報収集プログラム自体が、当然のことながら、新しいデータに対する需要をますます高めていく。そして、いったん情報が収集されると、それを標的に対して利用しなければならないという強い圧力がかかる。

次にあげるの弾圧方法はすべて、FBIや支援組織がCOINTELPROの一環として、あるいはCOINTELPROの標的に対して使用したものです。

1. 直接暴力

前記のフレッド・ハンプトン殺害は、FBIとシカゴ警察の共同作戦でした。フレッド・ハンプトンは、1960年代後半から1970年代にかけて、黒人の保護と支援プログラム（無料の朝食や診療所など）の提供を目的とした革命的社会主義の政治組織、ブラック・パンサー党（BPP）の議長を務めていました。BPPには、FBIによって「黒人ナショナリストのヘイトグループ」というレッテルを貼られ、COINTELPROの対象に含まれていました。ハンプトンの暗殺は、以下のような他の弾圧方法に支えられていました。

- **秘密裏の監視**　FBIから報酬を受けていた潜入者がもたらした情報によって、ハンプトンの襲撃と殺害が可能となった。
- **欺瞞**　同じ潜入者がBPPの他のメンバに濡れ衣を着せることでBPP内に不信と疑惑の雰囲気を作り出した。
- **マスメディアの影響**　ハンプトンが暗殺された後、BPPのメンバーは「民衆の悪魔」として描かれるなど、メディアの表現はますます歪められていった。

2. 法制度

共産主義者でブラックパンサー党員であり、COINTELPROの標的となったアンジェラ・デイヴィス[35]は、裁判所で判事が監禁・拉致され実行犯の逃走途中に警察との撃ち合いでその判事が死亡した事件について、デイヴィスが現場にいなかったにもかかわらず、カリフォルニア州で「加重誘拐および第1級殺人」の疑いで起訴されました。カリフォルニア州の検事は、誘拐犯らが使用した銃はデイビスの所有であり「犯罪を構成する行為を直接

35 (訳注)『アンジェラ・デイヴィスの教え 自由とはたゆみなき闘い』(河出書房新社)、『監獄ビジネス グローバリズムと産獄複合体』(岩波書店)、『もし奴らが朝にきたら 黒人政治犯・闘いの声』(現代評論社)、『アンジェラ・デービス自伝』(現代評論社)など。

行ったかどうかにかかわらず、犯罪の実行に関与するすべての者は、犯罪の主犯格である」と主張しました。当時、デイビスは所在はわかっておらず、J.エドガー・フーバーによってFBIの「最重要指名手配犯10人」にリストアップされました。数ヶ月後にデイビスは逮捕され、無罪判決が出されるまでの16ヶ月間を拘置所で待つことになりました。

3. 雇用の剥奪

デイビスは、法制度との闘いに先立つ1969年の就職1年目に、共産党員であることを理由にカリフォルニア州立大学機構で教えるのは不適当だとして、哲学教授の職を解雇されました。この解雇は、当時のカリフォルニア州知事ロナルド・レーガンの要請によるもので、レーガンは1949年に制定されたカリフォルニア州立大学において共産主義者の雇用を違法とする法律を持ち出たのです。このような法律の適用は、1940年代から1950年代にかけての「赤狩り」や「マッカーシズム」時代が終わっていないことを明らかにしました。FBIは、COINTELPROの前身であるCOMINFIL（Communist Infiltration）というプログラムで、労働運動、社会正義運動、人種平等運動の活動を内偵、追跡することによって、共産主義を悪とすることに加担しました。

4. 露骨な監視

COINTELPROについて初期に明らかとなったFBI文書の中に、"New Left Notes"と呼ばれる文書がありました。新左翼とは、1960年代から70年代にかけての幅広い政治運動のことで、市民権、政治的権利、女性の権利、同性愛者の権利、中絶の権利などの社会的問題に取り組む多くのグループを指します。「新左翼問題」への対処法について、このFBIフィラデルフィア支局のメモは次のように述べています。「これらの対象者や関係者にもっと尋問すべきだというのが、かなり一般的なコンセンサスであった。その理由は、これらのグループのパラノイアを増大させ、"郵便受けの背後には必ずFBI捜査官がいる"ことをさらに印象づることになるからだ。さらに、担当捜査官が圧倒的な個性をもって接触すれば、自分からすべてを話そうとする者も出てくるだろうし、継続して答える者もいるだろう。」

5. 秘密裡の監視

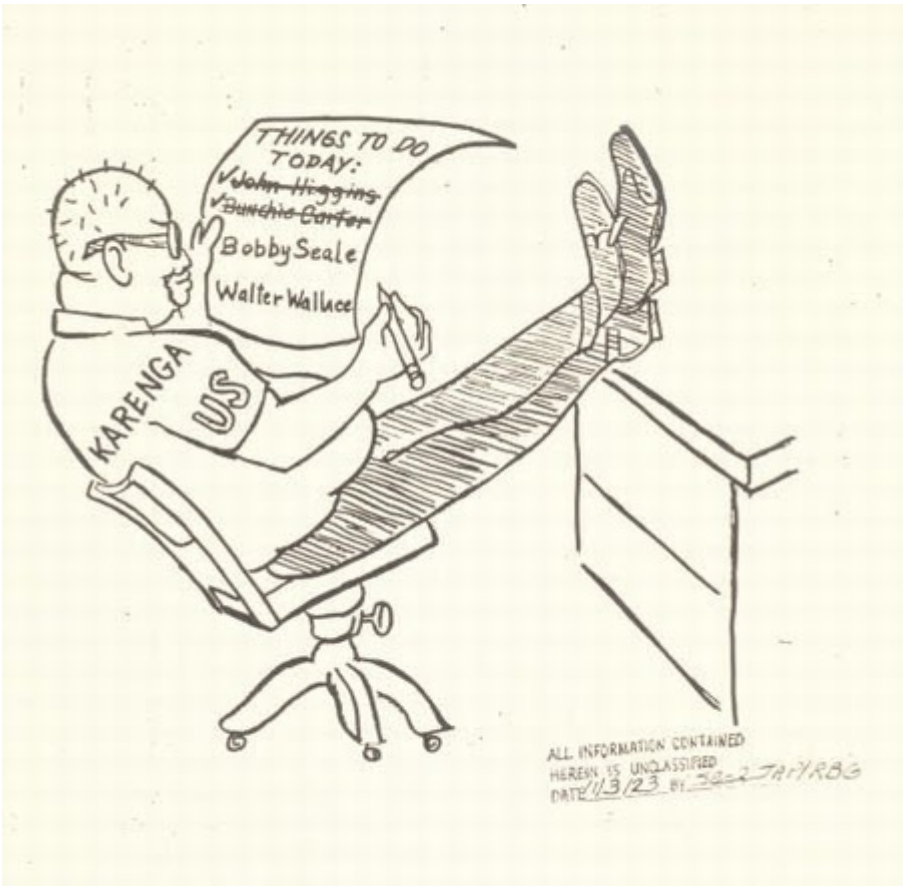
チャーチ委員会の報告書では、秘密裡の監視について、「範囲が非常に広いだけでなく、違法または不適切な手段で行われていることが多い」と報告しています。特に、CIAとFBIにはともに「郵便開封プログラム」があり、米国内の手紙を無差別に開封し、コピーを取るという行為を大規模に行っていました。その数はCIAによって1953年から1973年までに20万通以上、またFBIによって1940年から1966年までさらに13万通に及びました。しかも、CIAとFBIは、これらのプログラムのが続いていることについて、ニクソン大統領に嘘もついていました。

6. 偽装

FBI はしばしば偽の手紙やチラシを送り、グループの間で仲間割れをしかけました。下の写真は FBI が運動のメンバーをよそおって描いた漫画の一例で、黒人国家主義グループの「オーガニゼーション・アス Organization Us」（マウラナ・カレンガが共同で設立）とブラックパンサー党（BPP、著名なメンバーにヒューイ・ニュートン[36]、デビッド・ヒリアード、ボビー・シール、ジョン・ハギンズ、バンチー・カーターがいた）の間で暴力事件を挑発するためのものです。この漫画は、アスのカレンガが BPP を打ち負かしたことを示唆しています。後に FBI は、アスの何者かが 2 人の BPP メンバーを狙撃し殺害したことで、この作戦が成功だったと主張しています。

7.マスメディアの影響

マスメディアを操作することは、新左翼に対する FBI の COINTELPRO の明確な方針でした。チャーチ委員会によれば、「FBI のプロパガンダ活動の多くは、背後にいる FBI のことを確実に伏せておく“友好的な“メディアに情報提供することでした。FBI の犯罪記録部は、本部とメディアとの連絡を含む広報活動を担当していました。犯罪記録部は、その仕事（ほとんどが COINTELPRO とは無関係）の中で、“友好的な”報道機関、つまり FBI に有利な記事を書いてくれるメディアのリストを作成しました。また各地の支局はメディアの中に「秘密の情報源」（無給の FBI の情報員）を持ち、その協力を得ることができました。



暴力を扇動する FBI 漫画

36 『白いアメリカよ、聞け ： ヒューイ・ニュートン自伝』(サイマル出版会)

次に学ぶこと

社会運動に対するデジタルの脅威 監視と弾圧からの防衛

外部リソース

ボイコフ、ジュールズ Beyond Bullets: The Suppression of dissent in the United States. AK, 2007. カリフォルニア州オークランド。

ウィキペディア. “2019年 イランのインターネット・ブラックアウト” 2020年12月18日.

Shieber, Jonathan. “Zoom Admits to Shutting Đown Activist Accounts at the Request of the Chinese Government.” TechCrunch, June 2020.

Đuane de la Vega, Kelly, and Katie Galloway. “Eric and ‘Anna.” Field of Vision, November 19, 2015.

US Senate Select Committee to Study Governmental Operations with Respect to *Intelligence Activities and the Rights of Americans*. Report No.94-755. Washington, ĐC: US Government Printing Office, 1976.

Churchill, Ward, and Jim Vander Wall. *The COINTELPRO Papers: Đocuments from the FBI’s Secret Wars against Đomestic Đissent*. South End, 1990. Cambridge, MA.

図版の著作権者

暴力を扇動するFBI漫画 things-to-do 作成: Federal Bureau of Investigation、パブリックドメイン

社会運動に対するデジタルの脅威

「暗号化とは何か」 と 「メタデータ」の章を読んでおくことをお勧めします。本章と合わせて、「監視と抑圧から運動を守る」の章もお読みください。

この章で学ぶこと

1. 脅威モデルとは何か
2. 誰が監視を行っているのか、その戦略は何か

3．監視に使われる手段やプログラムの例

社会運動が権力者、権力組織、あるいは社会構造に挑戦するとき、広範囲にわたる監視リスクに直面します。ひとくちに脅威といっても、それが技術的にどのくらい洗練されているのか、脅威の可能性がどのくらいあるのか、被害の可能性がどのくらいあるのかには大きな違いがあります。**脅威のモデル化**とは、運動組織や個人が敵対する相手の範囲を検討し、様々なデータやデバイスが攻撃の犠牲になる可能性を推定し、攻撃された場合の被害についても検討するというプロセスをいいます。(そして、最もリスクが高く、失なわれたり外部へコピーされたりした場合に最もダメージの大きいデータの保護に努めます)。

ここでは、自分の身を守るために、次のような順序で監視について考えていきます。

●あなたの敵は誰か。ブラック・ライヴズ・マターの看板を庭に掲げたことであなたに復讐する近所のネオナチでしょうか。パイプライン反対運動を抑えようとする石油会社でしょうか、内部告発を阻止しようとしている米国政府でしょうか。敵対者が誰であるかを理解することで、敵対者のリソースと能力を推測することが可能になります。

●敵対者は特にあなたを追っているのか、あなたの正体を突き止めようとしているのか、それとも大量の情報を集めてそこからあなたに関する情報を得ようとしているのか。敵対者はどのような監視戦略をとっているのでしょうか。このような考察から、**どのような**データが、**どこで**危険にさらされる可能性があるのかを理解することができます。

●目的のデータを得るために、敵対者はどのような監視手段を採用するでしょうか。このことを知っておくと、そのデータを保護するには**どうすれば**いいのかを理解するのに役立ちます。

私たちは敵対者による監視リスクから検討を始めますが、これは戦略的にそうすべきだからです。完璧なデジタルセキュリティを実現することはできませんが、監視から身を守るためにどこに労力を費やすべきかを賢く判断することならできます。組織や社会運動における実際の脅威モデルの議論では、**誰が**潜在的敵対者かということは、その敵対者が**どのように**攻撃してくるかよりもはっきりしていることが多いのです。敵対者が誰であるかによって、利用しうる技術の範囲(利用可能なリソースや法的権限に応じて)が決まり、その結果、組織がどのような防衛行動や技術を採用できるかが決まります。

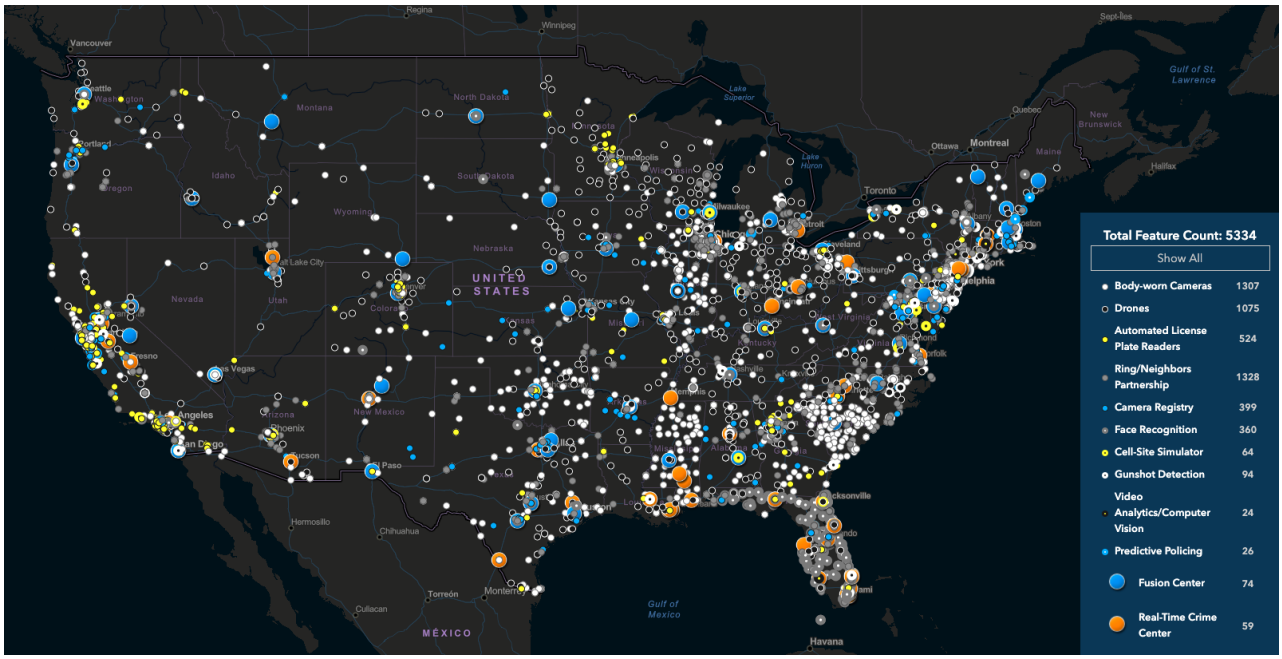
監視を仕掛けてくる敵対者

一般的に、敵対者はどのようなリソースを持っているかという観点から考えてみます。ここでは、敵対者を3つのカテゴリーに限定して考えます。

国民国家は、最も多くのリソースを持っているために監視能力が無限であるかのように見えます。それでも、強力な暗号を解読することはできないでしょう。ここでは、最も高度な監視能力を持つ組織として、米国家安全保障局(NSA)を考えてみます。2013年にエドワード・スノーデンが公開した情報は、国家レベルの能力を最も包括的に示すものであり、「スノーデン監視アーカイブ (Snowden Surveillance Archive)」で検索することができます。

大企業や地域の警察は、多くのリソースを持ち、互いに情報を共有していますが、必ずしも国家クラスの監視能力が使えるわけではありません。しかし、電子フロンティア財団の

Atlas of Surveillance のスクリーンショットに示されているように、監視を支援するテクノロジーは警察などの司法機関では広く使われています。



警察の監視技術の地図

敵対者が個人の場合は、リソースは少ないものの、あなたのことを知っているので、ソーシャル・エンジニアリングを使ってより効果的にデータを取得できる可能性があります。

ただし、リソースの少ない敵対者が利用できる技術は、リソースの多い敵対者でも利用できます。例えば、企業や司法機関は、情報提供者や潜入者を雇っていますが、これらの情報提供者は、あなた個人を知っている人かもしれません。また、より高度な監視能力は、通常、リソースの乏しい敵対者には利用できませんが、常にそうだというわけではありません。大都市の警察署が国家レベルの資源にアクセスできる場合もありますし（統合センター fusion center によるデータ共有など）、地元のネオナチが高度なハッキング技能を持っていて企業レベルの攻撃能力を発揮する場合もあります。

これらのカテゴリーは明確に分けられるものではありませんが、リスクを理解し、最も可能性の高い敵対者の戦略と、最も攻撃されやすいあなたの弱点を見つけるための出発点になります。

監視戦略

監視戦略には、大まかに分けて、「集団監視」と「標的監視」の 2 つがあります。

集団監視では、集団全体から情報を収集します。これは、その集団をよく知ることを目的として行われます。例えば、健康関連データを収集・分析することで、新たに発生した病気を特定したり監視したりすることができます。また、集団監視は、一群の監視対象者の中から対象となる人物を特定するための戦略として用いられることもあります。例えば、防犯カメラの映像を利用して、物的損害を与えた人を特定することができます。また、集

団監視によって、特定の個人に関する情報を収集することもあります。例えば、ナンバープレート・カメラを大量に配置して収集した情報をもとに、特定の個人の動きを追跡することができます。

標的監視は、個人または少人数のグループに関する情報だけを収集します。例えば、盗聴は、特定の個人の通信を傍受するものです。もっとも、警察などが誰かのメールを傍受するときは事前に正当な理由に基づく令状を取得する必要があり、ある程度確実な容疑が存在するときに監視が限られるはずで、憲法違反が横行しないように抑制されることにはなっています。

歴史的には、集団監視と標的監視とは明確に区別されていました。しかし、デジタル時代においては、後述するように、標的監視の手法が大規模に展開されることが多いのです。このような古典的な監視戦略の区分に加えて、私たちはデジタル時代に特有の広範な戦略に注目します。

Collect-it-all は、単純には大量監視の強化版と言えるかもしれませんが、これまで大量監視と言われたものをはるかに超えています。監視カメラや銀行取引の監視、電子メールのスキャンなどの大量監視に比べて、Collect-it-all はあらゆるデジタル化情報を吸い上げることを目的としています。さらに Collect-it-all は、ネットには送信されていない情報（個別接続された監視カメラの映像など）もデジタル化して収集するのです。Collect-it-all は、NSA の元長官であるキース・アレグザンダー将軍が提唱したことで悪名高いものです。彼の大量監視戦略は、9.11 以降にイラクで開始され、次のように説明されています。「干し草の山の中から一本の針を探すのではなく、彼のアプローチは『干し草の山全体を集める』というものでした。全部集めて、タグを付けて、保存して……そして欲しいものがあれば、それを探す」。エドワード・スノーデンが暴露した NSA のプログラムの多くは、このような発想から生まれたものと思われます。

敵対者が展開する監視戦略には様々な傾向があり、図のように、リソースの乏しい敵対者ほど戦略が少なくなる傾向にあります。

Adversary (Increasing Resources and Sophistication)	Surveillance Strategies: Targeted	Mass	Collect-it-all
Nation State	X	X	X
Corporation	X	X	
Individual	X		

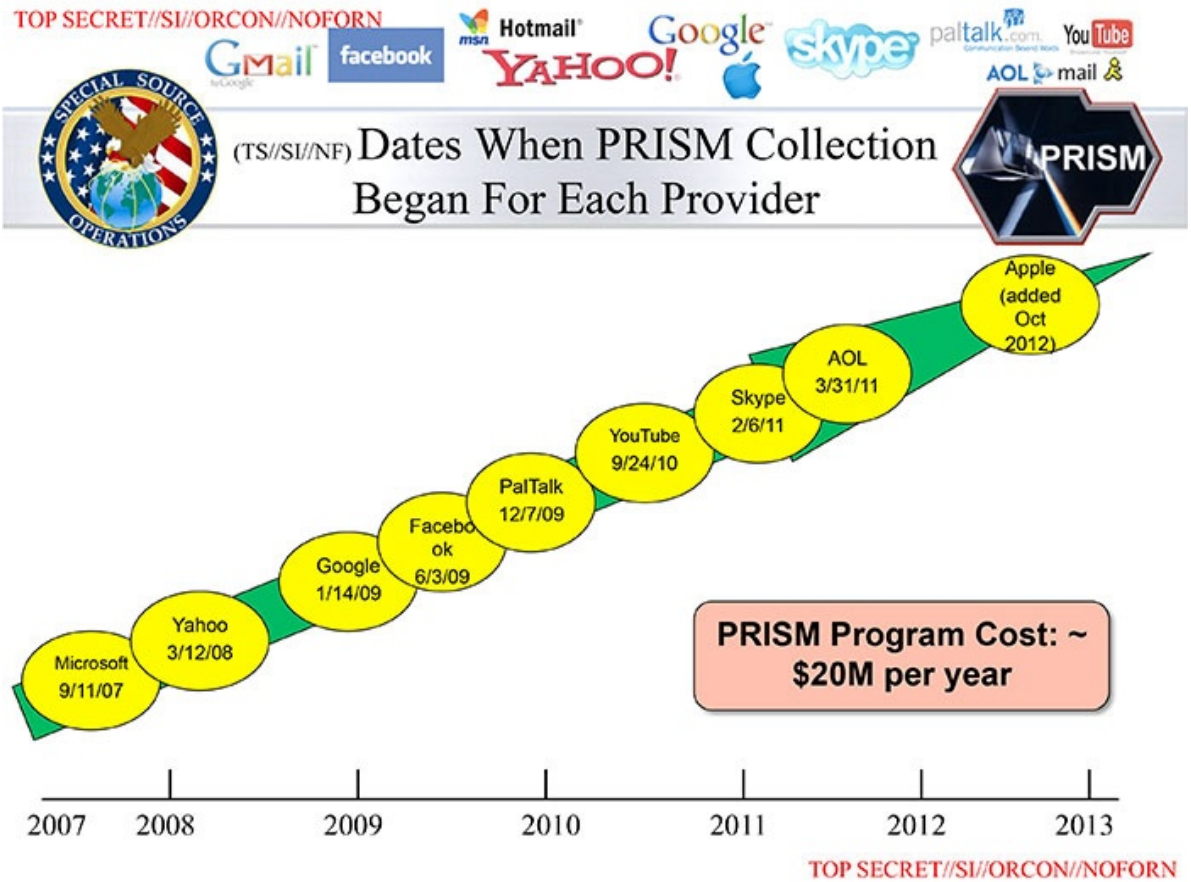
キャプション：敵対者とその監視戦略

監視戦術

あらゆるレベルの敵対者が利用できる監視戦術をすべて紹介すると、百科事典くらいの規模になってしまいます。ここでは、上記の監視戦略を支える監視プログラムとその戦術の例をいくつか紹介するにとどめます。以下では、これらのプログラムを使用するために必要な最低限の技能レベルと、これらの手段で情報収集される人の数に応じて、監視戦術を説明します。

大規模な傍受とデータの収集

まず、多くの人が大規模監視と聞いて思い浮かべるのは、膨大な量の通信を傍受し、記録することではないでしょうか。2013 年にエドワード・スノーデンが公開した情報の一部として、多くの大規模な傍受プログラムが明らかになりました。
STORMBREW、**FAIRVIEW**、**BLARNEY** の 3 つのプログラムは、NSA が通信会社と提携し、海底ケーブルを通過するデータをすべて収集するものです。これにより、暗号化されていないコンテンツと、それに関連するすべてのメタデータを、送信元から受信先までの移動中に収集することができます。ただし、電子メールやクラウドストレージ内のファイルなど、通信途上で一般的に暗号化されるコンテンツについては、これらのプログラムでは見ることができません。**PRISM** プログラムは、NSA とさまざまなインターネット企業（下図のように Google、Microsoft、Facebook など）が提携し、企業のサーバーに保管されているデータへ NSA がアクセスできるようにするものです。つまり、情報が送信中に暗号化されていて、STORMBREW、FAIRVIEW、BLARNEY で収集できない場合、NSA は PRISM を介して情報を入手することができます。ただし、協力企業のサーバー上でもユーザーが管理する鍵で情報が暗号化されている場合はこの限りではありません。



PRISM コレクション、米国家安全保障局

データの集約と分析

監視データを大量に手に入れたら、あなたならどうするでしょうか。巨大な干し草の山からちっぽけな針を見つけるなど、とてもできないでしょう。ここでデータマイニングが登場します。それには基本的な検索にとどまらず（怪しげな）機械学習予測モデルも含まれます。これによって敵対者は、膨大な量の大量監視データ（異なるソースからのものも含む）を役立てることができるのです。

最も基本的なのは検索機能です。つまり、大量のデータから、特定の人物に関連するデータなど、興味のあるデータを取り出すことができます。**XKEYSCORE** は、NSA が蓄えた大量監視データを対象とした Google ふうの検索機能を備えています。機能は基本的なものですが、アクセスできる情報の量が非常に多く（上で紹介した NSA のプログラムからの情報も含む）、XKEYSCORE（および関連するプログラム）は最も強力な敵対者だけが利用していると考えてよいでしょう。

一方、**Ðataminr** 社は、一般に公開されているデータ（ソーシャルメディアの投稿など）を検索し、自動（ソフトウェア）および手動（人間による分析）の両方の手段を用いて、新たに発生した“危機”（COVIÐ-19 の最新情報やジョージ・フロイドの抗議活動など）の詳細を明らかにし、報道機関、警察、政府などの顧客に提供しています。Ðataminr 社をはじめ、数十から数百はあるとされるソーシャルメディア監視プラットフォームは、憲法修正第 1 条で保護されている言論、特に Movement for Black Lives 連帯組織を監視していることで批判されています。Twitter や Facebook では、不正使用に対する世論の高まりを受けて、監視会社への自社のデータ提供を打ちきった例もあります。

また、**Palantir** は、特定の交差点、特定の地区、特定の個人など、どこで取り締まりすることが必要なのかを予測する多くの取り締まりプラットフォームの 1 つです。実際には、これらのプラットフォームはほとんど役に立たず、人種差別的な規範を強化するだけのものになっています。予測型取り締まりプラットフォームは、現在の警察データを出発点としており、過去に警察が取り締まりをした場所に警察官を派遣する傾向があります。しかし、有色人種のコミュニティや貧困地域は、特に過剰な警察活動が行われているため、予測モデルは、実際にそこで犯罪が発生しているかどうかと無関係に、単に警察を再びこれらの地域に送り込むことになります。

その上、2012 年から **EMBERS**（Early Model Based Event Recognition Using Surrogates）が「進行中の組織活動を検出し、それに応じて警告を生成する」ことによって、「世界の複数の地域」の「抗議行動、ストライキ、“オキュパイ”などの社会不安事象」を予測するために使用されています。この警告は完全に自動化されており、平均 9.76 日のリードタイム[37]で「いつ、どこで、どのような抗議活動が行われるのか（市の単位まで）」を予測することができます。ソーシャルメディアへの投稿、ニュース記事、食品価格、為替レートなど、一般に公開されているデータに全面的に依存しています。

標的を狙ったデータ収集

もう一つの監視手法として想起されるのは、盗聴です。しかし、現代の盗聴器は、昔のように電話線に取り付けるタイプよりも、はるかに簡単に使用できるようになっています。

37 （訳注） 予測から実際の事象発生までの時間。

その一つが CSS（Cell Site Simulator）で、これは、小型の基地局（ワゴン車に搭載されているくらいの大きさ）で、周辺の携帯電話は、この基地局からの電波が最も強くなるので、ここに接続します。最も単純な CSS でも、その地域の携帯電話の識別情報が明らかになります。(抗議行動の現場で携帯電話を使用している場合を想像してみてください。)CSS にも様々あり、それぞれ機能が異なります。CSS の中には、携帯電話とネットワークとの間ので通信を単純に受け渡ししながらも、その間にメタデータを読み取るものもあります。あるいは、例えば 3G から GSM へとサービスをダウングレードすることで、サービスプロバイダとの間で行われる携帯電話通信の暗号化を解除し、メッセージの内容にアクセスできる CSS もあります。さらに別の CSS は、携帯電話が CSS に接続してきたら、ネットワークには情報を渡さないようにすることで、携帯電話の通信をブロックすることができるものがあります。CSS は、冒頭の地図にあるように、警察などの機関はかなり多く保有しています。

また、CSS や高解像度ビデオカメラなどの監視機器は、監視用のドローンと呼ばれる無人航空機（**UAV**）に搭載することができ、監視範囲を数地区から街全体へと大幅に拡大することができます。これは、ターゲットを絞った監視の手法を、大規模の集団にまで拡大する一例です。Persistent Surveillance Systems 社は、米国の多くの警察署に UAV の使用を提案しました。Persistent Surveillance 社の UAV は、超高解像度のカメラを使用し、32 平方マイルの範囲で個々の車や人の動きを追跡したうえ、履歴を保存できるので、過去にさかのぼって動きを追跡することができます。

もちろん、密かに情報を収集する必要がない場合もあります。丁寧にお願いすればそれで情報を収集できることもあります。米国では、民間のプロバイダーに情報を要求するために、召喚状や令状が用いられます。[38]令状には（法的な意味での）正当な理由が必要ですが、召喚状には必要ありません。Google は透明性報告書で公表しているように、毎年約 4 万件のデータ要求を受けており、そのうち約 3 分の 1 が召喚状によるものです。Google は、データ要求の約 80％でデータを渡しており、各要求では平均して 2 つのユーザーアカウントが影響を被っています（つまり、個々のデータ要求は高度に標的化されているということです）。[39]注目すべきは、電子メールの内容が召喚状によって入手できるということです。召喚状や令状は技術的には単純なものですが、通常は敵対者の中でも政府レベルだけが使用できるものです。

デバイスへの攻撃

上記の手法は、通信途上またはクラウドに保持されているデータを収集しようとするものです。しかしデータを収集する最高の場所は、あなた自身のデバイス（携帯電話やコンピュータ）です。これは、勾留や捜索に際して警察があなたのデバイスを押収した場合に起こる可能性があります。この点については、「デバイスの保護」の章で詳しく説明しますが、ここでは、デバイスに保存されているデータを取り出すいくつかの手法を紹介します。

Cellebrite 社はイスラエルの企業[40]で、携帯電話その他のデバイスからデータを抽出するためのツールを専門に販売しています。**UFED**（Universal Forensic Extraction Device）

38 （訳注）日本の場合は、裁判所の令状の他に、刑事訴訟法第 197 条第 2 項に基き、「公務所又は公私の団体に照会して必要な事項の報告を求めることができる」ことから、「捜査関係事項照会」が用いられる場合がある。

39 （訳注）日本の場合、Line は、捜査機関からのユーザー情報開示・削除要請の件数を公開している。2020 年 7 月から 12 月で 1571 件の要請があり、そのうち 75 パーセントに応じている。
https://linecorp.com/ja/security/transparency/2020h2

は、ブリーフケースに入れて持ち運べるほど小型で、ほとんどの携帯電話から素早くデータを抽出することができます。ただし、これにはデバイスを物理的に管理下へ置くことが必要です。NSO グループ（これもイスラエルの企業）は、一部の iPhone やアンドロイドに **Pegasus** というスパイウェアを遠隔操作でインストールし、テキストメッセージや通話のメタデータ、パスワードなどのデータを抽出する機能を売りにしています。NSA は、データを収集したり、データがターゲットデバイスに到達するのをブロックしたりすることができる **QUANTUM** と呼ばれるマルウェア（悪意のあるソフトウェア）を一揃い保有しています。NSA は、自身のサーバーを Facebook サーバーなどに偽装し、ターゲットの端末にマルウェアを仕込む手段として利用する **TURBINE** システムを用いて、この悪意のあるソフトウェアを大量にインストールすることができます。

Pegasus と QUANTUM は広範に展開することが可能ですが、これらのプログラムは一般に世論の反発を招くため、政治的には危険な場合があります。侵入タイプの監視技術は広く展開するほど、Pegasus がそうであったように、発見され易くなるのです。

個人的な嫌がらせ

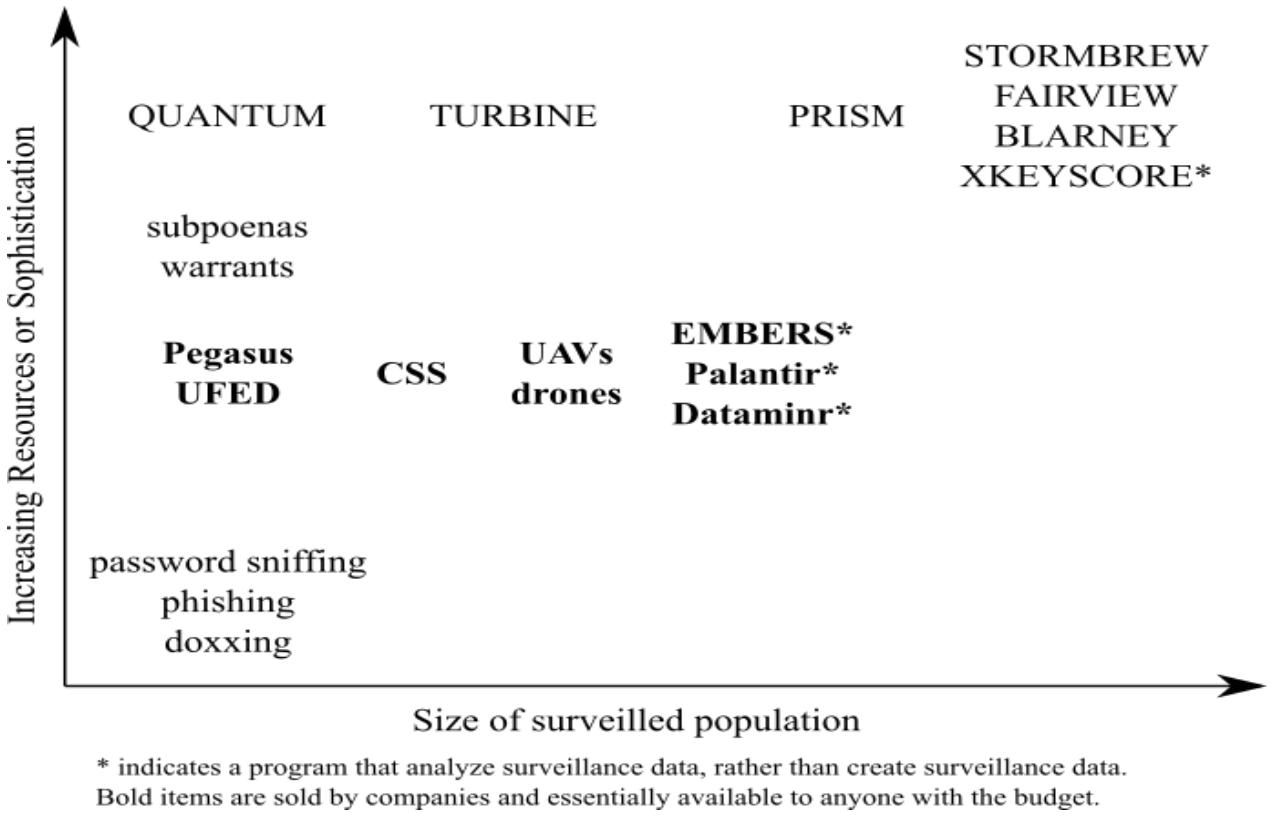
典型的な監視の領域とは異なりますが、デジタルセキュリティのリスクを考える際には、個人的な嫌がらせも念頭に置く必要があります。Ðoxxing、フィッシング、パスワード・スニッフィングは、リソースの乏しい敵でも利用可能な技術で、無視することはできません。「パスワード」の章で紹介したブラック・ライヴズ・マターの活動家デレイ・マッケソンは、2 要素認証を採用していたにもかかわらず、Twitter のアカウントを侵害されたという話を思い出してください。その敵対者は何らかの個人情報を知りたがっていたのですが、公的な情報源や個人的な知識からわかったかもしれません。

Ðoxxing とは、標的となる人物の個人情報をディスカッションサイトなどで公開し、標的となる人物に危害を加えたり、困惑させたりすることを意味します。これはとても簡単にできることですが、一方であなた自身を守ることは非常に困難です。いったん自分に関する情報がオンラインで公開されると、それを削除することは困難または不可能です。

フィッシングとは、偽装された電子メールや Web サイトを通じて、パスワードなどの個人情報を入手する方法のことです。フィッシングは大規模に展開されることもありますが、最も成功しているタイプはスピアフィッシング spear phishing です。これは標的の個人についてすでに知られている情報を利用し、成功率を高めるやりかたです。

パスワード・スニッフィングは、あなたがパスワードを入力するのを肩越しに見るようなローテクなものから、キー・ストローク・ロガーをインストールしてあなたがパスワードを入力するキーボード操作を記録するようなものまであります。キー・ストローク・ロガーをあなたのデバイスへインストールするためには、それだけの技術力が必要ですが、さまざまなうまい方法があります。また従来タイプのパスワード・スニッフィングでは、ネットワークを通過中のパスワードをキャプチャします。これは通信が暗号化されていない場合に可能であり、これも様々なレベルの技術が必要ですが、熟練した個人であれば可能であることは間違いありません。

40 （訳注）日本のサン電子が買収し、子会社となっている。
https://www.sun-denshi.co.jp/company/abroad/



* indicates a program that analyze surveillance data, rather than create surveillance data.
Bold items are sold by companies and essentially available to anyone with the budget.

*印は、監視データを生成するというよりも監視データを分析するプログラムです。太字のアイテムは企業が販売しているもので、購入資金があればだれでも可能なものです。

コンテクスト：スタンディングロック

2016年、石油を送るダコタ・アクセス・パイプライン（DAPL）の建設に反対する人々が、建設予定のミズーリ川とキャノンボール川の合流地点に抗議行動用の“ベースキャンプ”を設置しました。このパイプラインは、スタンディングロック・インディアン居留地をはじめとする多くのネイティブ・アメリカンのコミュニティを含む地域の飲料水の水質を脅かしていました。最終的にベースキャンプは数千人の規模になり、10ヶ月間にわたって活動を続けました。

DAPLを建設しているEnergy Transfer Partners社は、民間の警備部隊を雇い、抗議活動が開始されて数カ月後には、抗議者たちに攻撃犬を差し向けたりしています。さらに、Energy Transfer Partners社は、抗議運動が始まるとすぐにそれを鎮圧のためTigerSwan社を雇っていました。TigerSwan社は、対テロ戦争時に米国政府の委託を受けてアフガニスタンで活動を開始した民間の傭兵会社です。それだけにTigerSwan社は軍隊式のテロ対策を採用しており、抗議するネイティブ・アメリカンの人々や彼ら支援者たちを反乱分子と呼び、TigerSwan社設立時の相手であったジハード主義者の戦闘員とみなすという明らさまな態度を示しました。TigerSwan社の監視活動は、ソーシャルメディアの監視、空中からのビデオ撮影、無線の盗聴、潜入者や情報提供者の利用など多岐にわたっていました。

抗議に対して州当政府や連邦政府の治安組織が呼び込まれる段階になると、TigerSwan社はFBI、米国国土安全保障省、米国司法省、米国連邦保安局、インディアン局(the Bureau of Indian Affairs)と定期的に連絡を取りながら、州や地方の警察に状況報告を

行っていました。TigerSwan 社が採用している戦術の多く（すべてではないですが）は、政府の法執行機関が採用すれば違法なものですが、州は民間企業から最新情報を受け取るという方法で法の網の目をくぐっています。これは、法執行機関の多くが一般的に行っていることで、警察は、国が直接収集した場合には修正第 4 条に違反するようなデータを民間保有データとして購入しています。

州の法執行機関、Energy Transfer Partners 社、それに TigerSwan 社の“官民協同事業”は、抗議活動のベースキャンプを終息させるのに効を奏しました。最終的に州政府は、催涙ガス、震盪手榴弾、放水（氷点下の天候で）を使って抗議する人々を暴力的に排除した結果、約 300 人が負傷しました（片腕を失いそうになった女性をいます）。

ベースキャンプは排除されパイプラインが完成に向かう一方で、反対運動は続き、最終的には裁判所から「新しい環境影響評価を行うために、パイプラインは停止し、石油を抜かなければならない」という判決が出されました。

集団監視は、ほとんどすべての人の情報を集めるにもかかわらず、それがもたらす害には差があることを覚えておく必要があります。特定のグループがより厳密に監視されたり、特定のグループに関しての監視情報がとても頻繁に利用されたりします。アメリカで国や企業の監視によって不均衡な被害を受けているグループの例としては、イスラム系アメリカ人、黒人（アフリカ系アメリカ人）、アメリカ先住民、そして 「社会運動抑圧のメカニズム」の章で説明したように、社会運動の参加者が挙げられます。

次に学ぶこと

あなたのデータがどのように収集されるかという説明が続いたので気分が下がってしまったでしょう。すぐに「監視と抑圧からの防衛」の章をお読みください。

出典

表現の自由のためのカナダ人ジャーナリストのグループ. “Snowden Surveillance Archive”. Accessed February 9, 2021.

Electronic Frontier Foundation “Atlas of Surveillance.” Accessed February 9, 2021.

国土安全保障省. “Fusion Centers.” アクセスは 2021 年 2 月 9 日。

Google. “Transparency Report.” Accessed February 9, 2021.

Nakashima, Ellen, and Joby Warrick. “For NSA Chief, Terrorist Threat Drives Passion to ‘Collect It All.’” Washington Post, July 14, 2013.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* London: Hamish Hamilton, 2015.

N, Yomna. “Gotta Catch ’Em All: Understanding How IMSI-Catchers Exploit Cell Networks.” Electronic Frontier Foundation、2019 年 6 月 28 日。

Stanley, Jay. “ACLU Lawsuit over Baltimore Spy Planes Sets Up Historic Surveillance Battle.” American Civil Liberties Union, April 9, 2020.

Biddle, Sam. “Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr.” Intercept, July 9, 2020.

Ahmed, Maha. “Aided by Palantir, the LAPD Uses Predictive Policing to Monitor Specific People and Neighborhoods.” Intercept, May 11, 2018.

Muthiah, Sathappan, Anil Vullikanti, Achla Marathe, Kristen Summers, Graham Katz, Andy Doyle, Jaime Arredondo, et al. “EMBERS at 4 Years: Experiences Operating an Open Source Indicators Forecasting System.” In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining-KDD ’16, 205–14. San Francisco: ACM, 2016.

Boot, Max. “Opinion: An Israeli Tech Firm Is Selling Spy Software to Dictators, Betraying the Country’s Ideals.”. Washington Post, December 5, 2018.

Intercept,“Oil and Water.” 2016-17.

Fortin, Jacey, and Lisa Friedman. “Dakota Access Pipeline to Shut Down Pending Review, Federal Judge Rules.” New York Times, July 6, 2020.

図版の著作権者

警察の監視技術の地図 atlas-of-surveillance © Electronic Frontier Foundation is licensed under a CC BY (Attribution) license

敵対者とその監視戦略 surveillance-strategies © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

PRISM コレクション、米国家安全保障局 prism_slide_5 © JSvEIHmpPE は, Public Domain ライセンスの下で提供されています。

監視戦術 surveillance-tactics © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

Part3：反対運動を防衛する 社会運動を守るために（アメリカ編) – 反監視情報

監視と抑圧から身を守る

本章をお読みになる前に、「社会運動抑圧のメカニズム」と「社会運動に対するデジタルの脅威」の章をお読みになることをお勧めします。

この章で学ぶこと

1．脅威モデルとは

2．デジタル・セキュリティへの脅威を減らすための戦略

完璧なデジタル・セキュリティは存在しないと言われていますし、私たちもそう思います。十分なリソースを持った敵の監視能力はほぼ無限であり、「社会運動に対するデジタルの脅威」で説明した現実も、ほんの一部を紹介しただけなのです。それでも、リスクがすべて同じわけではないし、あらゆる監視ツールも同じように使用されるわけではなく、個人やグループが監視による脅威を軽減するためにできることはたくさんあります。
デジタル・セキュリティへの脅威は、次のような関係でモデル化できます。

$$\text{threat} \propto \frac{(\text{surveillance capabilities}) \times (\text{suppression risk})}{\text{effort required to obtain data}}$$

このモデルでは、**監視能力(surveillance capabilities)**とは、「社会運動に対するデジタルの脅威」の章で説明したように、相手のリソースのレベルを指します。**抑圧リスク(suppression risk)**とは、「社会運動抑圧のメカニズム」の章で述べたように、相手がどのようにしてあなたを弱体化させようとするかということです。[41]
留意すべきは、監視が間接的にも直接的にも抑圧を支えるということです。「社会運動抑圧のメカニズム」の章で紹介した例の多くは、実際に監視によって支えられています。例えば、

● ブラックパンサー党のリーダーであるフレッド・ハンプトンを狙って暗殺という**直接暴力**が実行された前提には、彼のスケジュールやアパートの間取りについての詳細な情報がありました。

● 米国司法省は、ドナルド・トランプ大統領就任式への抗議行動を組織した者に対して、**法的制裁**を加えると脅し、行動組織のウェブページすべてのトラフィック情報の取得を要求しました（「アノニマス・ルーティング」の章の最後に記載）。

● スティーブン・サライタ Steven Salaita の**雇用剥奪**は、彼の Twitter での活動の監視によるものでした。

41 （訳注）分母の「effort required to obtain data」は、「データを取得するのに必要な努力」を意味する。

● モハメド・モハムド Mohamed Mohamud に対して FBI が行った**謀略**は、モハムドの電子メールを監視することから始まりました。

脅威を軽減すること

デジタル・セキュリティの脅威を減らすには、監視能力や抑圧のリスクを減らすか、★自分のデータを得るために敵側が費やす労力を増やすことが有効です。

監視能力を低下させる

活動家はふつう、監視機能をすぐにコントロールする手段を持ち合わせていません。しかし、一部の州や市で顔認証や CSS を禁止するなど、監視を規制する優れた取り組みがいくつかあり、一定の成果を上げています。とはいえ、社会運動の目的が監視の禁止や制限にあるのでなければ、このような取り組みは当初の運動の目的から外れてしまいます。

弾圧のリスクを減らす

同様に、活動家は弾圧のリスクもほとんどコントロールできません。運動が敵への圧力を減らせば弾圧リスクも最小限に抑えることはできますが、それでは萎縮効果に屈することになります。

データ取得にかかる労力を増やす

私たちに残されているのは、あなたのデータを取得するための労力を増やすことであり、これが本書が焦点にしている課題です。相手があなたのことを知れば知るほど、あなたを弱体化させることができるので、あらゆるデータを保護することは重要ですが、データを保護するために必要な努力は、最も保護が必要なデータに絞ることが戦略的には好ましいのです。そのためには、相手の監視能力と、相手があなたの努力を抑えようとする方法を念頭に置き、次のようなデータの保護に注力するのです。

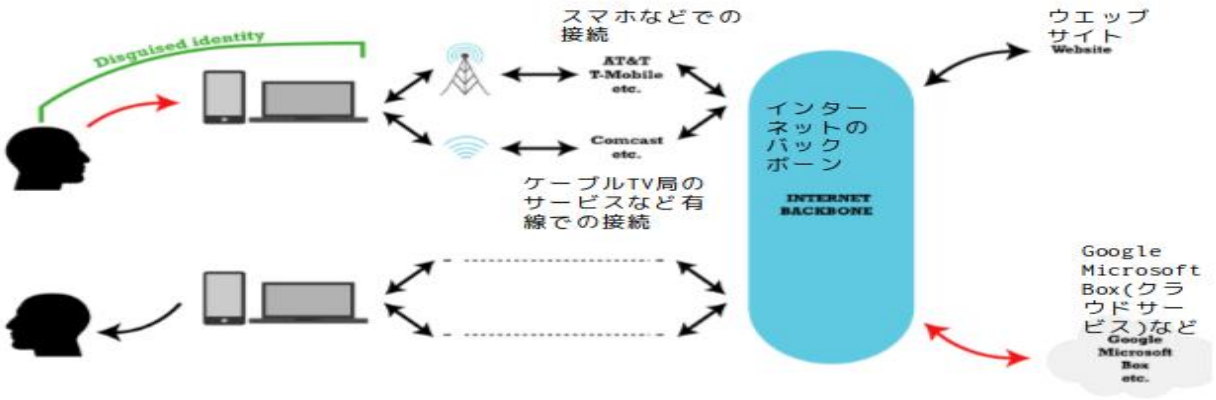
1．あなたの活動を抑圧するために使用される可能性が高く、しかも、

2．監視に対して最も脆弱なデータ

ポイント 1 を理解するには、個別の社会運動の取り組みとその敵を深く理解する必要があります。ポイント 2 を考えるためには、自分のデータがどこにあるのか（以下で説明）、それをどうやって保護するのか（この後の各章で説明）を理解する必要があります。

あなたのデータはどこに？

データの脆弱性がどこにあるかによって、あなたのデータ保護戦略が変わります。あなたの情報は、デバイス（携帯電話やノートパソコンなど）に入れられた時点でデータとなり、一部はその後、サービスプロバイダーを経由してインターネット上に送信されるでしょう。ここでは、あなたが閲覧するウェブサイトと、あなたのデータが保管される可能性のあるクラウドプロバイダー（Google や Facebook など）とを区別しておきます。



あなたデータの保管場所

以降の章で、あなたのデータが置いてある場所を保護する方法について説明していきます。まず「セキュリティ文化」の章では、自分の情報をデータにするかどうか（それを自分でコントロールできる場合）、データをクラウドに保存するかどうか、つまりデータを左の赤い矢印の方向に転送するのかについて決める方法を説明します。「デバイスを守る」の章では、自分が管理しているデバイス（ノートPCや携帯電話など）に保存されているデータを保護する方法について説明しています。「通信を守る」の章では、自分の手元からウェブサイトやクラウドプロバイダー、その他の通信相手にデータが送信される途中のデータを保護する方法について説明します。「リモートデータを守る」の章では、あなたがクラウドを利用することにした場合に、クラウドに保管されているデータを保護する方法について説明します。

さらに、「アイデンティティを守る」の章では、自分のアイデンティティを保護する方法、つまり、オンライン上で匿名または偽名を使い、検閲を突破する方法について説明します。最後に、結論として、デジタル・セキュリティ・ツールをどのように選択すべきかを述べ、私たちが実際に使っている推奨原則も紹介します。

コンテクスト：エドワード・スノーデン

2013年までの数年間、エドワード・スノーデンは、システム管理者としてアクセスしていた職場（主にNSAの下請け企業）のデータを収集しました。スノーデンが大量の機密情報をリークしたことで、世界で多くの強力な政府が行っている監視戦術がいかに高度で広範囲に展開されているかが明らかになりました。しかし、このような情報を公開するために、スノーデンは国家安全保障局という強力な敵に立ち向かうことになりました。

スノーデンはずっと匿名でいられるなどと思っていませんでした。そこで彼は、自分の行動（情報収集）と目標（内部告発）をなるべく長い間知られないようにしながら、責任を持って報道してくれるジャーナリストに情報をリークし、できれば自由に暮らせる安全な場所にたどり着くのに十分な期間を確保することにしました。スノーデンは、グレン・グリーンウォルド（大胆不敵で徹底した取材で知られるジャーナリスト）と暗号化された通信チャネルを設定するのに数ヶ月を要しました。これはエンド・ツー・エンドで暗号化されたメッセージングアプリが「プラグ・アンド・プレイ」で使えるようになる前の時代でした。しかし、スノーデンの情報公開に関する報道が始まると、彼は自分の正体がバレることを知り、自ら仮面を外しました。スノーデンは、希望していた場所（ラテンアメリカ）にはたどり着けませんでした。香港（グレン・グリーンウォルドにリードを開示し

た場所）からロシアへのフライト中にアメリカのパスポートが取り消され、それ以上の空の旅ができなくなってしまったのです。スノーデンはロシアに亡命することができました。

しかし、スノーデンの内部告発は非常に成功し、その報告はその後何年も続き、私たちのコミュニケーションに数々の変化をもたらしました。今では暗号化がより一般的になり、多くの人は自分の会話がエンド・ツー・エンドで暗号化されているときでさえ気づかないほどになっています。

次に学ぶこと

セキュリティ文化

外部リソース

AnarchoTechNYC. “Persona Based Training Matrix“.

2020年6月9日電子フロンティア財団. “Your Security Plan.” Surveillance Self-Defense, August 1, 2014.

Snowden, Edward J. Permanent Record, 2019.Metropolitan Books.

出典

あなたデータの保管場所 WHERE-YOUR-DATA-IS © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) license

セキュリティ文化

本章を読む前に、「監視と抑圧から身を守る」の章を読むことをお勧めします。
この章で学ぶこと

1. 社会運動のセキュリティ文化とは何か

2. デジタル・セキュリティにセキュリティ文化が不可欠な理由

国家や民間の敵による密告者を使った弾圧の歴史を知っている社会運動では“セキュリティ文化”と呼ばれるものが発展しています。この言葉は、グループとその活動、グループのメンバーや幅広い社会運動に対する侵入や監視などの抑圧的な脅威による悪影響を最小限に抑えることを目的とする情報共有の方法や行動上の注意事項を意味します。つまり、ここでの“セキュリティ”は、デジタル・セキュリティよりもはるかに広い意味を持ちます。文化という言葉は、セキュリティの原則と実践が即座の対応可能な直感的なものになることへの期待を示しています。理想的なセキュリティ文化とは、グループが安全で容易にコミュニケーションをとることができり、必要に応じて新しいメンバーを迎え入れることができる一方で、過剰な被害妄想や煩雑な手続きやポリシーを避けることを可能にするもです。

セキュリティ文化に対する考え方や実践方法は様々ですが、次の重要な原則は広く採用されていて、ぜひ守りたいものです。

1. 情報は知る必要があるものだけを共有する。

2. 一緒に組織を作る場合、できるだけグループのメンバーをよく知ること。

3．ゴシップやうわさ話を避ける。

セキュリティ文化とデジタル・セキュリティの接点

ここでは、これらの要素をデジタル・セキュリティとの関連性について詳しく見ていきましょう。

知る必要について：情報の共有とデジタル化を最小限に抑える

秘密を守るための第一の原則は、信頼しなければならない人の数を最小限にすることです。もちろん、情報の機密性には濃淡があり、公開ミーティングの告知や準備段階でのプレスリリースもあれば直接行動の具体的な場所と時間など、様々なものがあります。どのような情報を保護する必要があるかを決定し、それを守るために注意を払うことは、全体の一部に過ぎず、それに加えて、仕事をする上で必要な場合でなければ機密情報を知ってはいけないということを、だれもが理解する必要があります。

デジタル・セキュリティの観点からは、どのような情報をデジタル化するかを決めることも重要です。（本当に抗議活動に参加する予定の人たちをリストアップしたGoogleドキュメントが必要なのか。本当にデモに参加した人たちの写真を掲載する必要があるのか。本当にこれらの投稿が公開されるべきなのか、公開すれば地理的な位置が特定されるでしょう。） 情報共有の量と範囲を制限することは、優れたデジタル・セキュリティ対策と密接に関係しています。なぜなら、完全に安全なプラットフォームやコミュニケーション手段は存在しないからです。

具体的なデジタル・セキュリティ対策（複雑なエンド・ツー・エンドの暗号化技術の使用など）を講じる前に、どのような情報を保存し、共有し、そもそもデジタルで保存する必要があるのかについても考えてみてください。たぶん、今のような世界的パンデミックでなければ、私たちは可能な限り直接会って私たちの考えていることを議論すべきでしょう。デジタル情報はとにかく、コピーが非常に簡単です。どれほど強力な暗号化を施しても、情報にアクセスする人を信頼できる程度までしか情報を保護できないことを覚えておいてください。たとえ完璧に設計された安全なアプリやデジタル・プラットフォームであっても、グループへの侵入者や離反者による情報の漏洩を防ぐことはできません。

知るということ：交流と信頼の構築

一緒に仕事をする人のことをよく知り、予測されるリスクにも共に立ち向かえる関係を築いていくことが理想的です。しかし、情報をデジタル化すると、組織の中枢により多くの「関係者」（それには企業や国家も含まれます）を迎え入れることにもなります。例えば、グループのメンバー間のコミュニケーションにGmailを使用している場合、Googleはそれらの電子メールをすべて保有しており、それらの電子メールは国家によって簡単に収集される可能性があります。このように、データが暗号化されていないときは、そこへアクセスできるのが人間であろうと、インターネット・サービス・プロバイダーであろうと、クラウド・ストレージ・プロバイダーであろうと、メールプロバイダーであろうと、すべての対象についての信頼性を確認しておく必要があります。

ゴシップやうわさ話をしない

これまでにいろいろな社会運動がゴシップや噂によって潰されてきました。「社会運動抑圧のメカニズム」の章で説明したように、ゴシップや噂に惹かれてしまう人間の弱点を国家は有利に利用してきました。濡れ衣・挑発者・虚偽プロパガンダといった騙し戦術が使われ、その情報を信じた社会運動のメンバーが情報拡散する、といったことが起きました。

デジタル・セキュリティという目的では、情報源の確認がよい指針となります。これが特に重要となる理由は、デジタルでは発信者の偽装がローテクな手段（偽アカウントやアカウントの盗用など）やハイテクな手段（ネットワークトラフィックのリダイレクトなど）を使って簡単にできるためです。デジタル情報源の確認については、「通信を守る」の章と、終章の「デジタル・セキュリティ・ツールの選択」で説明します。

ここでとても重要な注意点は、ソーシャルメディアの利用についてです。そこにはゴシップや噂が氾濫しており、個人の生活の詳細が知られ、弱点を探るためにわざわざプライバシーへ侵入する必要などないほどです。ソーシャルメディアのプラットフォームは情報を公開するためにのみ使用すべきであり、そこでの会話を決してプライベートなものと考えてはいけません。

これらの保護措置は、ソーシャルメディアの監視、捜査機関の召喚状や捜査令状、そしてdoxxing（晒し、バラし）からあなたを守る一歩となります。

コンテクスト： セントポール原則

ミネソタ州セントポールで開催された2008年の共和党全国大会に向けて、イラク戦争を支持する共和党への反対を中心に、さまざまな社会運動が集結しました。抗議団体の連合体では、大会に先立ち、各グループの見解や戦略の自由を守り、あるグループが直面しているリスクが他のグループに影響を与えるのを避けるために、次の4つの原則を採択しました。

1. 私たちは連帯の基礎を、戦術の多様性と他団体の計画への尊重においている。
2. それぞれの行動や戦術は、時間的・空間的に分離されるように組織される。
3. 議論や批判は運動の内部にとどめ、仲間の活動家やイベントを公開の場やメディアで非難しない。
4. 私たちは、国家による監視、潜入、破壊、暴力など、反対意見の弾圧に反対する。私たちは、活動家やその他の人々に敵対する法執行機関の活動には協力しない。

これらのルールは、「セントポール原則」として知られており、これ以降、多くの連合体で採用されています。この原則によって、セキュリティ文化の概念はグループ内のものからグループ間のものへと拡大されたのです。この原則は、異なるグループが同じ目標を持っていながらそこに到達するための方法で意見が異なる場合であっても、これらのグループが一緒に活動することを支え、運動体が共通に掲げた全体的目的が達成に一層近づくことを目的としています。

次に学ぶこと

・デバイスを守る

・通信を守る

・アイデンティティを守る

外部リソース

ウィキペディア.“2008年共和党全国大会”2021年1月11日

Activistsecurity.org. A Practical Security Handbook for Activists and Campaigns. Civil Liberties Ðefense Center, May 2007.

Sprout Anarchist Collective. “What Is Security Culture?” 2012.

デバイスを守る

本章の前に「パスワード」と「社会運動へのデジタル脅威」の章を読むことをお勧めします。

この章で学ぶこと

1.携帯電話やコンピューターが危険にさらされる一般的な状況

2.携帯電話やコンピューターを守るための戦略

携帯電話やノートパソコンに保存されているデータは膨大です。連絡先、電子メール、写真、文書、カレンダー、確定申告書、銀行口座情報、そしてスマホの場合は、携帯電話を持っている間の位置情報の詳細な履歴も含まれています。これらのデータの多くは、クラウドストレージプロバイダー（Apple、Google、Ðropbox など）とも共有されますが、これについては「リモートデータを守る」の章で説明します。ここでは、ラップトップや携帯電話に保存されているデータを、遠隔地からの攻撃や実体的な攻撃から守ることに焦点を当てます。

実体的攻撃

実体的攻撃とは、紛失、盗難、没収などにより、敵対者がデバイスに直接にアクセスすることを意味します。善良な人ではなくて敵の手に渡るかもしれないような場所で、携帯電話を紛失したり、敵が携帯電話を盗んだりするかもしれません。さらに、国境を通るときや、逮捕された際に携帯電話が没収される（計画的かどうかを問わず）こともあるでしょう。

2017 年 1 月 20 日のアメリカ大統領就任式への抗議活動（J20）で大量逮捕に巻き込まれた人たちはスマホを没収され、スマホはイスラエル企業 Cellebrite 社のツールによる検索の対象となりました。Cellebrite 社のツールはデバイス（スマホやパソコン）の情報すべてと、そのデバイスがアクセスしているリモートアカウント（Google、Facebook、Ðropbox など）をすべて抽出します。How to Protect Yourself from the Snitch in Your Pocket（ポケットの中の密告者から身を守る方法）」という記事の中で、ある J20 の被告は、没収された携帯電話から Cellebrite 社のツールによって 8,000 ページにも及ぶデータが抽出されたと述べています。以下の情報は、弁護の準備中に弁護士から彼が得たものです。

●私に連絡してきた電話番号や電子メールを含むすべての連絡先のリストで携帯電話に保存されていなかったもの。私が彼らに電話をかけたり、メッセージを送ったり、電子メールを送ったり、彼らから電話をかけられたり、メッセージを送られたりした回数がカウントされている。

●特定のメールアドレスとの送受信メール、下書きメールの数と、それらのメールアドレスと共有していたカレンダー登録のイベントの数。それぞれの電話番号からの着信/発信/不在着信の数、相手が私の連絡先に登録されているかどうか、登録されている場合は携帯電話でどのようなニックネームで呼んでいるか。私と相手の間の総通話時間。

●ある番号との間の受信/送信/下書きされた SMS テキストの数。削除された場合でも、下書きを含むすべてのテキストの内容。

●Whatsapp の連絡先、その「ユーザー名」（アカウントに登録されている電話番号）、および私とその人との間のチャットや通話の回数。

●すべてのアプリ、インストール／削除／最後に使用／購入した時期、およびそのアプリが持つ権限。

●Google Ðrive に保存されていたオーディオファイル、ポッドキャスト、ボイスメモ、着信音など。作成／削除／変更／最終アクセスのタイムスタンプ。

●すべてのカレンダーイベント、招待された参加者、位置タグなど。

●一般的な通話ログ情報・携帯電話が中継局に接続した日付／時刻／位置、Google マップにリンク。携帯電話がアクセスしたすべての携帯基地局を示す世界地図。

●Signal、WhatsApp、SMS、Google ハングアウト、TextSecure、GroupMe などでのチャット全部と、Google Ðocs、それらチャットの参加者全員のリスト、テキスト本文、既読か未読か、送信と既読のタイムスタンプ、スター付きかどうか、削除されたかどうか、すべての添付ファイル。これらのチャットには、スマホを使い始める前のものも含む。

●連絡先のすべての情報。削除されたかどうかも含めて。

●ウェブブラウザのクッキー。

●テキスト文書、添付ファイル、Google ドキュメント、アプリで作成されたものなど、スマホで開いたすべての文書。

●電子メールおよび電子メールの下書き（すべての送信情報、本文テキストの全部、16 個までの添付ファイル、を含む）。

●画像/写真/動画、作成/アクセスされたタイムスタンプ、およびすべてのメタデータ。

●Twitter アカウントのひとつから、ランダムなツイート 96 件（古くは 2013 年のものを含む）

●携帯電話が接続したことのあるすべての無線 LAN ネットワークのリスト、そのパスワード、ハードウェア識別子、接続した日時。

●携帯電話の電源を入れた直近の 5 回（没収されてから 2 ヶ月後の 2 回を含む）。

●ウェブ履歴とウェブおよび Google Play ストアの検索履歴。

●携帯電話に入力されたすべての単語と、その単語が何回入力されたかのリスト（単語としてのメールアドレスや、自動修正されないように辞書に追加した単語も含む）。

●いわゆる「タイムライン」：メール、通話、電子メール、ウェブ履歴、地図検索を含むアプリの使用、無線 LAN ネットワークへの接続や新しい中継局への接続など、すべての行動が順に並べられるようにタイムスタンプ付きで。

どうすべきか？

J20 の裁判で証言した刑事は、暗号化を有効にしていた携帯電話でアクセスできたのは基本的なデバイス情報に限られ、携帯電話内の記憶装置の内容にはアクセスできなかったと述べています。最新の OS を搭載している iPhone や Android 端末は、デフォルトで暗号化が有効になっていますが、Apple や Microsoft のパソコンでは暗号化を有効にする設定が

必要です。しかし、デバイスの暗号化は万能ではありません。そのデバイスで暗号化に設定されたパスワードの強さの程度まで保護されるだけなのです。

デバイスを暗号化するときのパスワードは、残念ながら利便性と安全性のトレードオフの関係にあります。パスフレーズ（「パスワードについて」の章に説明があります）は、実体的な攻撃に耐えるために 6 つ以上の単語でできたものがよいのですが、そのようなパスフレーズを頻繁に入力するのは面倒です。対策はいくつかありますが、いずれもトレードオフの関係があります。携帯電話やノートパソコンの場合は設定を変更すれば、パスワードやパスフレーズやロック解除コードを入力する頻度を変えることができます。[42]（暗号化の効果があるのは、画面のロックが有効化されているときだけです。）また、パスワードやパスフレーズやロック解除コードの強さ（長さ）を使用する状況に応じて変えておくこともできます。ただし、これらの方法を実行するには、高いセキュリティが必要となる状況をいつも予測し、それに応じたセキュリティ対策をとり続けることが必要です。

携帯電話や一部のノートパソコンでは、パスフレーズの入力に代えて指紋などの生体情報を入力することができます。指紋はパスワードを入力するよりも便利です。ただし暗号化のためには指紋と結びつけたパスフレーズを使用することになります。（そのパスフレーズは実際的範囲でできるだけ強くしておくべきです）。しかし、法執行機関によってデバイスが没収された場合、指紋も強制的に取られる可能性があります。そのため、デバイスが没収されるリスクが高い場合は、やはり生体認証によるロック解除機能はオフにしておくことを検討すべきでしょう。

また、実体的な介入に対する保護策の強化も考えられます。プライバシーフィルムを貼っておけば、入力したパスワードやその他の情報を盗聴者に見られないようにすることができます。ファラデーバッグ[電波遮断バッグ]は、携帯電話が情報を送受信するのを防ぐことができます。特に、携帯電話が位置情報を記録するのを防ぐことができます。携帯電話のリモート・ワイプ機能[43]は、主要な携帯電話メーカーが提供しています。この機能は、あなたの情報を敵と共有する可能性のある企業にあなたのデバイスの情報や操作を委ねることになるかもしれませんが（「リモート・データを守る」の章に説明があります）、状況によっては有用なツールとなるかもしれません。

リモート攻撃

リモート攻撃とは、インターネットやデータ接続を介して携帯電話やノートパソコンのデータに敵対者がアクセスすることを意味します。デバイス（スマホを対象とすることが多い）にマルウェアを感染させる機能を設計・販売している企業があり、その顧客（つまりあなたの敵対者、それが企業や国家のエージェントであっても）があなたの情報の一部または全部にリモートアクセスできるようにします。

「社会運動に対するデジタルの脅威」で紹介したように、シチズン・ラボ Citizen Lab ではイスラエルの NSO グループが開発・販売しているスパイウェア「Pegasus」が広範囲に渡って使用されていることを発見しました。このスパイウェアは、標的にされた人がリンクをクリックするように仕向けるソーシャル・エンジニアリングと組み合わせることで、携帯電話のカメラやマイクをオンにして録画・録音したり、通話やテキストメッセージ（エンド・ツー・エンド暗号化が施されているものも含む）を記録したり、GPS の位置情報を記録したり、これらの情報をターゲットの敵対者に送り返したりすることができます。

42 （訳注）たとえば一定時間操作をしないとロックされて、再度パスワードを入力することが必要になるように設定することができる。このロックまでの時間を 1 時間にするのか 5 分にするのかではセキュリティのリスクが 5 分の方が高くはなるが頻繁にロック解除のパスワードを入力しなければならない。

43 （訳注）携帯電話やスマートフォン、ノートパソコンなど持ち運び型の情報端末に記録されているデータを、通信回線を通じた遠隔地からの指示により消去すること。また、端末の持つそのような機能。（IT 用語辞典）

シチズン・ラボは、アラブ首長国連邦の人権擁護者である Ahmed Mansoor 氏が、またメキシコでは政府の汚職を告発している政治家や甘味飲料への課税を主張する科学者など 22 人がターゲットとなって Pegasus が試みられたと報告しています。

何ができるのだろうか？

NSO グループが販売しているようなリモート攻撃は、ゼロデイと呼ばれるコンピュータソフトウェアの欠陥を利用しています。このような欠陥は、ソフトウェアの提供者（Apple や Microsoft など）が発見しておらず、それが判明するとき（0 日目）まではソフトウェアの提供者がその脆弱性を修正したりパッチを当てたりすることがないため、被害者が自分自身を守ることはできません。コンピュータ・セキュリティは、しばしば「いたちごっこ」です。NSO グループのようなマルウェアやスパイウェア開発者の製品は、ターゲットが（より正確には、提供者である Apple、Google、Microsoft などの企業が）マルウェアの開発を知らない間だけ有効です。なぜなら、マルウェア攻撃が判明すればすぐに製品を修正してマルウェアを無効化するからです。

しかし、そのような修正は、ターゲットとされるあなたがデバイスのソフトウェアを更新した場合にのみ、機能します。つまり、ここでの教訓は、セキュリティ更新がダウンロード可能になったら、すぐにもれなく更新をインストールすることです。残念ながら、スマホは無期限にセキュリティ更新が提供されるわけではなく、あるデバイス（例えば Nokia 5.3）が OS（例えば Android）でサポートされる期間は数年に限られています。Apple や Android の携帯電話がセキュリティ更新されているかどうかは、“設定”で確認することができます。

マルウェアの多くはフィッシングによって、ターゲットのデバイスにインストールされます。つまり、メールかテキストメッセージをターゲットに送りつけて“説得”し、リンクをクリックさせたり、ファイルを開かせたりします。そのため、次にできることは、クリックするときは十分に注意することです。差出人を知っていますか？その送信者から何が届くことになっていますか？何か怪しいことはないですか？実際に Ahmed Mansoor がスパイウェアの感染を避けることができたのは、警戒心があったからです。彼がフィッシングメールをシチズン・ラボに送ったことから、NSO Group がスパイウェアを悪用していることがわかったのです。

最後にひとこと、インストールするアプリと、そのアプリに与える権限に注意してください。懐中電灯アプリが連絡先やカメラにアクセスする必要があるでしょうか。 また、無名のソフトウェア開発者が作成したゲームをインストールする必要があるでしょうか。インストールしたアプリはどれもがマルウェアを媒介する能力を持ちうるので、ミニマリズムを実践する良い機会となります。

コンテクスト：デモ参加者の携帯電話を危険にさらす

2020 年 9 月、オレゴン州ポートランドで 2020 年夏に行われた大規模な抗議活動の際、国土安全保障省が「参加者の携帯電話から情報を抽出していた」ことが明らかになりました。政府は、携帯電話のクローンを作るという斬新な方法を用いて、デモ参加者の携帯電話への通信を傍受したとされています。これは危険な動きであり、おそらく違法でしょうが、この攻撃の詳細は秘密とされています。しかし攻撃方法を推測し防御を強めることはできます。

もしこういったクローン作成に実体的な攻撃が必要だった場合は、その夏の逮捕に際して没収されていた携帯電話を対象にした可能性が高いでしょう。しかしそれでは監視対象が逮捕者の携帯電話に限られる上、逮捕者は自分の携帯電話を信用しないことにしたり、工場出荷状態にリセットして潜んでいるかもしれないマルウェアを排除することもできます。

一方、遠隔操作だけでクローンを作ることができれば、侵害する携帯電話の数を大幅に増やすことができ、没収の必要もなく秘密裏に実行できます。

いずれの場合でも、「通信を守る」の章で説明したように、通信経路とエンド・ツー・エンドの暗号化を使用することで、携帯電話の通信を保護することができます（ただし、メタデータは必ずしも保護されません）。

次に学ぶこと

・通信を守る

・アイデンティティを守る

外部リソース

Earth First! The Journal of Ecological Resistance. “How to Protect Yourself from the Snitch in Your Pocket”（ポケットの中の密告者から身を守る方法）2017-18 年冬号。(この記事のデジタル版は protestarchive.org でご覧いただけます)

Marczak, Bill, and John Scott-Railton. “The Million Ðollar Ðissident: NSO Group’s iPhone Zero-Ðays Used against a UAE Human Rights Ðefender.”[The Million Ðollar Ðissident: UAE の人権擁護活動家に対して使われた NSO グループの iPhone ゼロディ] Citizen Lab, August 24, 2016.

Schiano, Chris.“Criminalizing Ðissent: Contested Evidence Introduced in J20 Trial Testimony.” Unicorn Riot, [Criminalizing Ðissent: J20 裁判の証言で紹介された争点となる証拠”. ユニコーン・ライオット]November 30, 2017.

Klippenstein, Ken. “Federal Agencies Tapped Protesters’ Phones in Portland.” Nation, September 21, 2020.

Vice Media Group. “Phone Crackers.” 2021 年 2 月 9 日に確認。

通信を守る

本章をお読みになる前に、「中間者」、「パスワードについて」、「社会運動に対するデジタルの脅威」の各章をお読みになることをお勧めします。

この章で学ぶこと

1.通信経路の暗号化とエンド・ツー・エンド暗号化の違い

2.暗号化しないと、誰があなたの情報にアクセスできるか

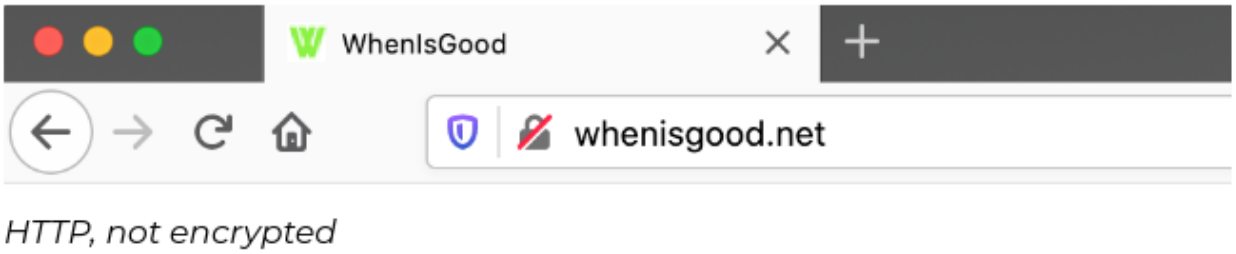
3.暗号化すると、誰があなたの情報にアクセスできるか

4.エンド・ツー・エンド暗号化した場合、誰があなたの情報にアクセスできるか

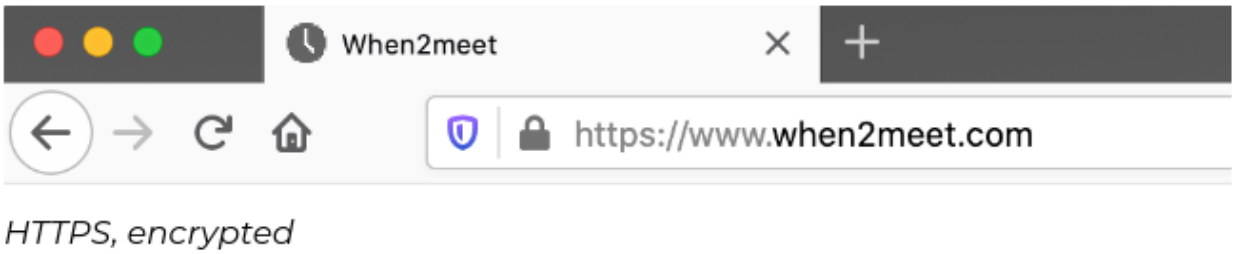
オンライン・コミュニケーションを保護する最善の方法は、暗号化です。しかし、どんな暗号化でも同じように保護できるわけではありません。ここでは、保護の度合いを区別する概念に焦点を当てます。

暗号化されているかどうか

暗号化通信の最も基本的なバージョンは通信経路の暗号化です。このとき、あなたのコンピュータとサーバーの間であなたの情報が暗号化されています。ウェブを閲覧する場合、通信の内容を敵から保護するには、この方法が最も適しています（ただしメタデータは保護されません）。ほとんどのウェブブラウザでは、暗号化されているかどうかが以下のようにアドレスの枠のところへ示されています。



HTTP, not encrypted

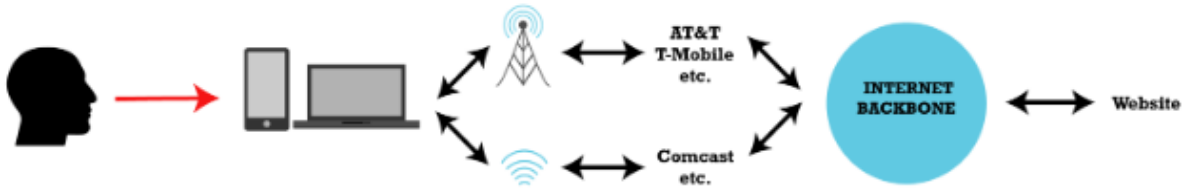


HTTPS, encrypted

(上図)HTTP、暗号化されていない（下図)HTTPS、暗号化されている

上の最初の例では、情報は暗号化されずに送信されています。この場合の URL の全体は `http://whenisgood.net` では、`http` は暗号化されていない Web ページへのアクセスを意味します。このブラウザ（Firefox）では、この点を強調するために、閉じた南京錠アイコンには取り消し線が表示されています。下側の例では、情報が暗号化されています。`https` は暗号化された Web ページへのアクセスを示し、末尾の s は“secure”を意味しています。この暗号化に使用される鍵は、「暗号化のための鍵の交換」の章で説明したように、ディフィー・ヘルマン鍵交換を使用して、あなたのコンピュータと `when2meet` のサーバーとの間で交換されます。

`http` を使用すると、下図のようにあなたとウェブサイトの間の経路上にある者はだれでも、あなたが閲覧しているウェブのコンテンツ（読み込まれた画像やウェブフォームに入力された情報など）にアクセスできます。さらに、これらの経路上の機器間の通信（プロバイダのネットワークとインターネットバックボーン間の通信など）を盗み見している人も、あなたの閲覧内容にアクセスできる「可能性」があります。ここでの可能性の意味は、この経路上の 2 者間の通信が暗号化されている場合があるからです。例えば、携帯電話と基地局の間の通信は、ほとんどの場合、暗号化されています。

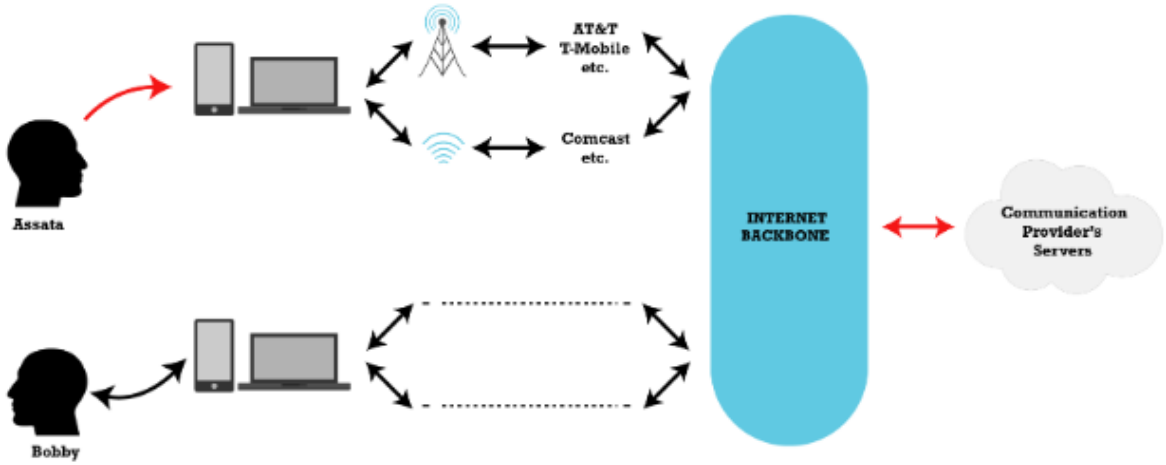


誰があなたの閲覧データにアクセスできるのか

一方、https を利用した場合、あなたの閲覧**コンテンツ**にアクセスできるのは、あなたとウェブサイト（厳密にはウェブサイトをホスティングしているサーバー）のみです。ここでコンテンツと表現したのは、あなたとウェブサイトの間の経路上にある者たちが、ウェブサイトの基本 URL、あなたがウェブサイトを閲覧した時間、ウェブサイトからダウンロードした情報の量など、特定のメタデータを知りうるからです。

データ転送中の暗号化

私たちが電子メール、インスタントメッセージ、ビデオチャットなどで他の人と通信するとき、これらのコミュニケーションは（ほとんどの場合）、以下の図のように、通信プロバイダー（例えば、電子メールの場合は Google のサーバー、Skype 通話の場合は Microsoft のサーバー）を経由して行われます。現在では、それらの通信は通常、暗号化されていますが、ほとんどの場合、あなたと通信プロバイダーの間でのみ暗号化されています。つまり、Assata と通信プロバイダーのサーバー（センター）の間や、通信プロバイダーのサーバーと Bobby の間の経路にある盗聴者や通信機器を運用する業者は、あなたの通信内容にはアクセスできませんが（ただし、メタデータは取得できます）、通信プロバイダーはあなたの通信内容にアクセスできるのです。



誰がユーザーの通信データにアクセスできるか

Assata と通信プロバイダー、通信プロバイダーと Bobby の間を行き来する間にコンテンツが暗号化されることから、これをデータ転送中の暗号化 `in-transit encryption` と呼んでいます。通信経路での暗号鍵は、下図のように、アサタとボビーの間の経路の各部分で別々に生成されます。通信プロバイダー（中央）は、アサタとの間でディフィー・ヘルマン鍵交換を行って共有鍵を生成し、ボビーとの間では別のディフィー・ヘルマン鍵交換を行っ

て別の共有鍵を生成します。アサタがプロバイダを介してボビーにメッセージを送信する際には、まずアサタがプロバイダと共有する鍵でメッセージを暗号化し、その後プロバイダにメッセージを送信します。プロバイダは、アサタとプロバイダが共有する鍵でメッセージを復号化します。次に、プロバイダは、プロバイダがボビーと共有する鍵でメッセージを再暗号化してからボビーに送信します。ボビーはそのメッセージを解読することができます。したがって、メッセージが復号された状態で存在するのは、アサタとボビーのデバイスと通信プロバイダのサーバー上に限られており、ユーザーとサーバーなどの間を移動する際には、メッセージは暗号化されています。

データ転送中の暗号化

エンド・ツー・エンドの暗号化

データ転送中の暗号化は、インターネット・サービス・プロバイダ、Wi-Fi ホットスポット、通信経路上の盗聴者など、多くの潜在的な敵から通信を保護しますが、通信プロバイダは依然としてすべての情報にアクセスすることができます。たとえプロバイダが直接の敵でなくても、召喚状や令状がある場合などに敵と情報を共有する可能性があります。エンド・ツー・エンドの暗号化（E2EE）は、通信事業者からも通信を保護します。

E2EE（下図）では、アサタとボビーが鍵を交換します（ディフィー・ヘルマン鍵交換などの手順を使用して）。二人の通信は通信プロバイダを経由しますが、通信プロバイダが中間者攻撃を行わない限り、通信プロバイダを経由した通信は、ボビーとアサタだけがアクセスできる鍵で暗号化されます。つまり、メッセージは、アサタとボビーのデバイス上でのみ、復号された状態で存在します。アサタとボビーのデバイスはそれぞれ通信のエンドポイント呼ばれます（そのため、エンド・ツー・エンドの暗号化が行われたことになります）。

エンド・ツー・エンドの暗号化

認証

E2EE はとてもよい技法ですが、注意すべき点もあります。前述のように、エンド・ツー・エンドの暗号化は、通信事業者（または通信経路上の第三者）が、鍵交換の時点か

ら中間者攻撃を受けていない場合にのみ成立します。しかし、「中間者」の章で説明したように、アサタとボビーが独立したルートで鍵を確認すれば、中間者攻撃を受けていたかどうか、つまり通信が本当にエンド・ツー・エンドで暗号化されているのかを判断することができます。

E2EE を謳うアプリやサービスの多くは鍵の検証機能を提供していると主張する一方で、検証機能を提供しないものも多く、E2EE という主張を信用できる保証はほとんどありません。さらに、鍵を検証する機能を提供している E2EE アプリでも、ほとんどが新しい鍵をとりあえず信用するという Trust on First Use (TOFU) 方式で動作しています。つまり、最初に鍵を検証せずに通信を開始できるのです。しかし、それでも広範囲で自動化された中間者攻撃に対する防御は可能です。それというのも、実際に鍵の検証を行うことが E2EE を保証する唯一の方法である一方で、鍵を検証する機能があれば、ほんの一部のユーザーが鍵を検証すれば広範囲に及ぶ中間者攻撃が発見されやすくなるためです。

また、当然のことながら、E2EE はデバイス間の通信を保護するだけで、デバイス上のデータを保護するものではありません。アカウントやデバイスを保護するために、E2EE アプリに加えて強力なパスワードを使う必要があります。

コンテクスト：多人数のビデオチャット

2 人以上でビデオチャットをするためのアプリやサービスは数多くありますが、セキュリティの程度は様々です。ここでは、代表例を 3 つ紹介します。

●Wire は、E2EE の金字塔です。各ユーザーはアカウントを持ち、複数のデバイス (ノートパソコンとスマホなど) からアクセスできます。各デバイスごとに公開鍵があって、ビデオ通話などのセッションで暗号鍵を確立するために使用されます。これらの鍵のフィンガープリントを比較することで、真の E2EE を確認することができます。Wire は、12 人までのグループでの E2EE ビデオ通話が可能です。
●Zoom は、より大きなグループでのビデオ通話を可能にし、ユーザーが同じ鍵でビデオストリームを暗号化・復号化するという点で E2EE を提供します。しかし、この鍵は Zoom のサーバーによって確立され、配布されます。Zoom は暗号化キーにアクセスできるため、これは真の E2EE とは言えません。さらに、ユーザーが暗号鍵を検証する仕組みもありません。2020 年夏の時点で、Zoom は真の E2EE のための鍵を確立するための提案をしていますが、まだ実装されていません。
●Jitsi Meet も大人数でのビデオ会議を提供していますが、通信経路の暗号化のみを使用しています。しかし、Jitsi Meet はどのようなサーバーでも (その気になれば自分のサーバーで) ホストすることができます。社会運動に技術的なソリューションを提供し、多くのグループから信頼されている非営利団体、May First がホストしている Jitsi Meet のインスタンスがあります。May First はそこを使ったビデオ会議にアクセスでるのですが、Zoom のような営利企業よりも May First を信頼する人もいます。

次に学ぶこと

・デバイスを守る

・リモートデータを守る

・ユーザーのアイデンティティを守る

外部リソース

Blum, Josh, Simon Booth, Oded Gal, Maxwell Krohn, Julia Len, Karan Lyons, Antonio Marcedone, et al. “E2E Encryption for Zoom Meetings.”. Zoom Video Communications, Ðecember 15, 20E20.

図版の出典

HTTP、暗号化されていない http-example © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

HTTPS、暗号化されている https-example © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial)ライセンスの下に提供されています。

誰があなたの閲覧データにアクセスできるのか who-has-access-to-your-data © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial)ライセンスの下に提供されています。

誰がユーザーの通信データにアクセスできるか data-access-communication © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

通信経路の暗号化 notE2EE © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

エンド・ツー・エンドの暗号化 E2EE © OSU OERU は, CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

リモートデータを守る

本章を読む前に、「通信を守る」の章を読むことをお勧めします。

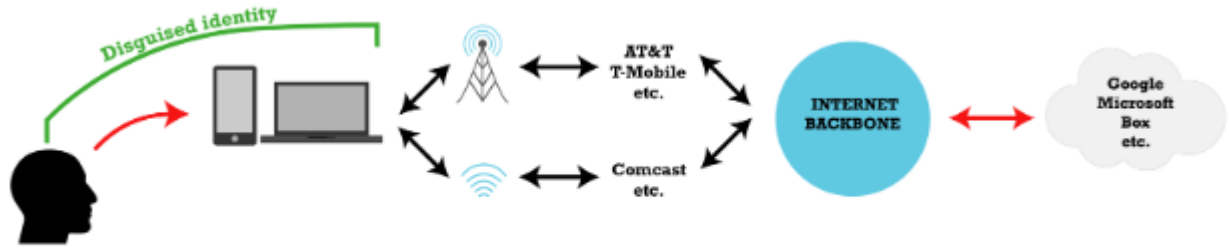
この章で学ぶこと

1.だれがクラウド上のデータにアクセスできるのか

2.どのようなデータがクラウドにあるのか

クラウドはどこでも使われています。2000 年代初頭から、データはあなたのデバイスだけでなく、デバイスや OS を管理している各企業のサーバーや、何かのサービス契約があればその会社のサーバーにも保存されるようになってきました (デバイス内にまったく保存しないこともあります)。このようなデータは、自分が管理する鍵で暗号化されていなければ、漏洩する危険があります。

クラウドに保存されたリモートデータへのアクセスは、以下の図のように Web ページへのアクセスに似ています。クラウドへのアクセス・モデルでは、ほとんどの場合、情報は通信経路の暗号化によって保護されており、デバイスからクラウド・ストレージ・プロバイダーのサーバーまでの経路で潜在的な敵からデータを保護します (下図)。



Who has access to your cloud data

誰がクラウドのデータへアクセスできるのか

しかし、「社会運動に対するデジタルの脅威」の章で述べたように、リモートに保存されている（そして暗号化されていない）データは、政府など敵対者が召喚状や令状によってアクセスできるほか、単なる第三者とも共有される可能性さえあります。残念なことに、最も明らかな形のリモートデータ保存（Dropbox や Google Drive など）を避けたとしても、私たちのデバイスの多くは、内部データ全体のリモートバックアップを推奨しており（Apple デバイスの iCloud など）、場合によってはそれを避けることが非常に困難です（Android デバイスの Google アカウントなど）。これらのデータには、アドレス、カレンダー、位置情報の履歴、閲覧情報など、あなたがコンピュータを使って行うあらゆる情報が含まれています。

コンテクスト：暗号化とクラウドストレージへの信頼

クラウドストレージには多くの選択肢があります。その例として以下のリストでは、暗号化されず信頼もできないもの、暗号化されていないが信頼してよいもの、暗号化されているものなど、オプションをいくつか説明します。

●Google は、あなたのすべての情報（メール、ファイル、連絡先、デバイスのバックアップ）を喜んで無料で保存します。もちろん、彼らはあなたのデータを利用することでそこから価値を引き出しますが、もしそのデータがあなただけが管理する鍵で暗号化されていれば、それはできません（だから暗号化していないのです）。「社会運動に対するデジタルの脅威」の章で見たように、Google は召喚状による請求のおよそ 80％に応じてデータを提供しています。
●ownCloud は、Box.com や Dropbox.com と似たクラウドストレージを提供するソフトウェアですが、Google の製品と同様に、通信経路の暗号化しか使用していません。(企業向けの ownCloud では、エンド・ツー・エンドで暗号化されたファイルの保存・共有が可能です。）しかし、ownCloud は、ビデオ会議アプリ Jitsi Meet のように、自分のサーバーを含むあらゆるサーバーでホスティングすることができます。また、Jitsi Meet のように、多くの人に信頼されているサービスプロバイダーである May First によってホストされている ownCloud のインスタンスがあります。May First がそこ保存されたデータへアクセスできるにもかかわらず、Google よりも May First を信頼する人もいます。
●CryptPad は、エンド・ツー・エンドで暗号化された Google Docs の代替となる共同編集プラットフォームです。ドキュメントは、復号化のための鍵を含むリンクによってアクセスできますが、その鍵は URL の#の後に表示されます。例えば、https://cryptpad.fr/pad/#/2/pad/edit/bpsky2zF5La8sZ_i-6r_cTj9fPL+ という URL の#の後の部分はフラグメント識別子と呼ばれ、サーバーには送信されず、ブラウザ内でのみ使用されます（この場合、特定のパッドを復号するために使用されます。暗号化キーは URL の一部であるため、このようなリンクを誰かに送る際には注意が必要です（例えば、Signal のような暗号化されたチャンネルでのみ共有する、など）。

●Keybase には、ownCloud や Dropbox のようなエンド・ツー・エンドの暗号化ストレージシステムをはじめとする様々な機能があります。CryptPad とは異なり、Keybase は（ブラウザではなく）専用のスタンド・アローン・アプリを使用し、鍵の管理を行います。

次に学ぶこと

パート 3 の残りの章

図版の著作権者

誰がクラウドのデータへアクセスできるのか Where-your-cloud-data-is © OSU OERU is licensed under a CC BY-NC (Attribution NonCommercial) ライセンスの下に提供されています。

自分のアイデンティティを守るために

本章を読む前に、「公開鍵暗号方式」と「匿名ルーティング」の章を読むことをお勧めします。

この章で学ぶこと

1.匿名性と仮名性の違い

2.Tor を利用する 3 つの方法

3.Tor を使うときに、やってはいけないこと

「匿名ルーティング」の章では、オンライン上で自分のメタデータを隠すための 2 つの方法として、仮想プライベートネットワーク（VPN）と Tor を紹介しました。これは、匿名性や仮名性を実現するのに役立ちますが、長期にわたって続けるのは難しいことです。本章では、VPN を介して Tor を利用するためのスキルを中心に解説しますが、これらの知識は VPN だけを利用する際にも応用できます。しかし、VPN を使用する場合、VPN プロバイダーはあなたが誰であるか、あなたのインターネット通信のメタデータを（さらに暗号化されていない場合はコンテンツも）知っているということをはっきり覚えておく必要があります。ここでは、Tor ブラウザを使った Tor の利用方法を中心に説明しますが、他のアプリケーションの場合も（セキュア・メッセージング・アプリケーションや OS 全体でさえも）、インターネットのリクエストを Tor ネットワーク経由で行うことができます。

匿名と仮名

Tor のさまざまな使用方法を説明する前に、匿名と仮名の違いについて考えてみましょう。これらの用語は文脈によって異なる意味で使用されますが、ここではオンラインでのコミュニケーションや行動に限定して使用します。

匿名とは、名前がないこと、もっと一般的に言えば、自分に結びつく識別子がないことを指します。あなたが今日、匿名でウェブサイトを訪れ、明日も同じウェブサイトを匿名で訪れた場合、ウェブサイトにはそれが 2 回とも同じ人であることを知ることさえできないはずです。ウェブサイトにわかるのは、"昨日は誰かが匿名でここを訪れた"、"今日は誰かが匿名でここを訪れた "ということだけです。

仮名とは、自分の正体をほとんど、あるいは全く知られていない状態で、別の名前を使うことです。例えば、サミュエル・クレメンズはマーク・トウェインというペンネームで本

を出版しましたが、もちろん出版社や一部の人々は本当の著者が誰であるかを知っていました。エドワード・スノーデンは、シンシナタスというペンネームを使ってジャーナリストのグレン・グリーンウォルドに連絡を取りました。グリーンウォルドは、誰がシンシナタスを名乗って連絡しているのか知らなかったし、スノーデンが連絡するときは Tor を使っていたので、グリーンウォルド以外の誰にも知られなかったのです。しかし、スノーデンがシンシナタスという別名を繰り返し使っていたことで、グリーンウォルドは (そしてジャーナリストのローラ・ポイトラスも) スノーデンから受け取ったさまざまな連絡を結びつけることができました。ここでは、仮名とは、1 つの人格のもとで、いくつもの、ときには匿名の通信セッションを結びつけることができることを指します。

Tor の使用方法

Tor はあなたの身元に関する情報(実際の場所など)を隠し、匿名性や仮名性を得るために使用することができます。初心者の場合、Tor Browser など Tor 方式に対応したアプリを使って Tor システムを利用します。上級者では、Tails や Whonix などの OS を使うとあらゆる通信が Tor 経由となり、もちろんウェブアクセスもすべて Tor 経由になります。

自分の位置を隠す

Tor ブラウザでは他のブラウザと同様に使用するだけで、あなたのユーザー名を使ったメールやソーシャルメディアへのアクセスを含め、あなたの物理的な位置をそれらのアカウントから隠すことができます。Tor ブラウザで新しいタブやウィンドウを開くたびに、そして一定の遅延の後に、Tor はあなたのウェブリクエストを新しい場所を経由してルーティングします。しかし、Tor を介してアクセスしているときがまさにそうなるのですが、異なる場所からアクセスされる場合、メールやソーシャルメディアのプラットフォームでは多くで、アカウントの挙動が疑わしいとしてフラグが立てられます。このように、Tor を常時、すべての用途に使用することは可能ですが、現実的ではないかもしれません。このような困難を乗り越えることができたとしても、実際の場所を隠しつづけるためにはさらに注意が必要で、以下のような行動は避けるべきです。

●ウェブサイトに住所などの個人情報を入力する、

●Word 文書や PDF などをダウンロードし、Tor ブラウザの外で開く。Word 文書や PDF などを含む文書の中には、写真など内容の一部をウェブ経由でアクセスする場合があります。こういった可能性のある文書をを開く必要がある場合は、インターネットから切断したあとで開いてください。

匿名性の確保

Tor を使えば匿名性が得られます。しかし、匿名性を損なうような情報を漏らさないように、注意して行動する必要があります。匿名性を維持するためには、実際の場所を隠す注意に加えて、匿名セッション中に以下のような行動を避ける必要があります。

●アカウントへのログイン (例：ソーシャルメディア、電子メール、銀行など)

●自分のウェブサイトを繰り返し表示する

仮名性の確立と維持

プレスリリースの投稿やフォーラムへの参加などのために、本名とは関係のないペンネームを作成した場合、ペンネームと本名とが関係ない状態を維持するために Tor が役立ちま

す。ただし、実名と仮名の区別を保つためには、以下のような行動を避ける必要があります。

●同じセッションで実名と仮名の、あるいは異なる仮名に対応するユーザー名にアクセスすること、これはこれらのアイデンティティを結びつけてしまうことがあります。

●Tor の外で仮名のアカウントに一度でもアクセスすること、

●電話機を使う二要素認証の使用（たとえプリペイド携帯電話であっても、あなたの現実の位置を明らかにすることができるからです。

●位置情報などのメタデータを含むメディアを投稿すること、

仮名のアイデンティティを長く使うほどミスを犯す機会が増えることに注意してください。上のようなミスに加えて、あなたの文体を分析することであなたを特定することができます。あなたの文体の例が多ければ多いほど（それが実名でも仮名でも）、あなたを特定することが容易になります。

Tor の警告

Tor を使ってインターネットにアクセスする際には、いくつか注意すべき点があります。

保護技術には完璧なものはありません。敵対者（エドガー）がアサタから Tor ネットワークへ入る接続と Tor ネットワークの出口でボビーのウェブサイトへの接続を監視することができれば、エドガーはアサタがボビーのウェブサイトを見ていると判断することができます。これをエンド・ツー・エンドのタイミング攻撃 end-to-end timing attack または相関攻撃 correlation attack と呼びます。

Tor 用に設計されていないアプリケーションを Tor ネットワーク上で使用しようとすると、画面の解像度や固有の設定などの識別情報が漏れる可能性があります。

最後に、Tor は匿名性を提供するだけであり、プライバシーを守るためには、https によるエンド・ツー・エンドの暗号化を使用したウェブページにアクセスする必要があることを覚えておいてください（残念ながら、すべてのウェブサイトがこれに対応しているわけではありません）。

コンテクスト：本物の Tor ブラウザを手に入れる

オンラインで自分を守るために使うツールは、本物でなければ意味がありません。2019 年、ビットコインを盗もうとしている（そして成功した）人たちによって、Tor ブラウザの偽バージョンが宣伝されていることが判明しました。彼らは悪意のある「Tor Browser」を、（正規のドメインである torproject.org ではなく）tor-browser[.]org や torproect[.]org などの不正なドメインで配布していたのです。誤ったサイトからダウンロードするようなミスや、悪意のあるアプリを提供する中間者攻撃から身を守るために、「Tor Browser」のようなアプリでは、「公開鍵暗号方式」の章で説明したように、ダウンロードの署名を確認することができます。

次に学ぶこと

パート 3 で未読の章があればお読みください。

外部リソース

Hancock, Alexis. “Phony HTTPS Everywhere Extension Used in Fake Tor Browser.” Electronic Frontier Foundation、2019 年 10 月 31 日。

Tails, 2021 年 2 月 9 日に確認。

Tor プロジェクト. “Tor Project: Overview.” 2021 年 2 月 9 日に確認。

Whonix. “Tips on Remaining Anonymous.” December 26, 2020.

Whonix. “Whonix: Software That Can Anonymize Everything You Do Online.” 2021 年 2 月 9 日に確認。

結論 デジタルセキュリティツールの選択

この章は最後にお読みいただくことをお勧めします。

この章で学ぶこと

コミュニケーションツールの評価と選択の基準

デジタル・セキュリティ・ツールには様々なものがあり、その中から選択できます。どのツールを使うかを決めるのは、とても大変なことです。私たちがツールを推奨する際には、ツールの提供者への信頼が少なくて済むものを選ぶようにしています。以下に挙げる**必須の基準**は、この点を考慮しています。また、**追加の技術的な基準**として、望ましいけれど必須ではないものを挙げています。最後に、ツールの提供者についての**技術以外の基準**もあり、無数の選択肢の中から決断を下す際に役立つでしょう。

例を挙げて説明するように、あるツールが完璧であることは稀です。それを使用するグループに適したツールを見つけることもまた選択過程の一部です。そのためには、たとえ必須の基準であっても、妥協しなければならないことがあります。また、すべての基準がすべてのツールに当てはまるわけでもないことにも注意してください。例えば、Tor Browser は匿名でインターネットを閲覧する機能を提供しますが、それだけではエンド・ツー・エンドの暗号化を目的としていないため、第一の基準に当てはまりません。

最後に、ツールは慎重に選択し、テストをしてから多くの人に採用を勧めてください。新しいものを使ったり、習慣を変えたりすることは社会的なコストといえますが、使い始めたツールがうまくいかないなど不要なコストは最小限に抑えたいものです。

必須の基準

1. **エンド・ツー・エンドの暗号化**（「通信を守る」の章で説明）により、信頼すべき当事者の数を最小限にするというセキュリティ文化の原則に従うことができます。エンド・ツー・エンドの暗号化により、ツール提供者からデータを守ることができます（ただし、メタデータについては必ずしもそうとは限りません）。エンド・ツー・エンドの暗号化を実装することは、社会運動の参加者に限らず、すべての人の権利を守るための、私たちの最優先の基準です。

2. ツールが**フィンガープリンティングによって連絡先の鍵を認証する機能**を提供している場合、「中間者」の章で説明したように、中間者攻撃を防ぐことができます。もしツールがこのフィンガープリンティング機能を提供していない場合、誰も知らないうちにツールの提供者が中間者攻撃を仕掛けている可能性もあります。

3．**オープンソースのクライアント**であれば、例えばエンド・ツー・エンドの暗号化が本当に強固に実装されているかどうかを、より広範なサイバーセキュリティの専門家コミュニティが検証することができます。ソースコードとオープンソースの意味については、「現代の暗号技術」の章で説明しています。クライアントとは、あなたのデバイス上で実行されるアプリのコードを意味し、プロバイダのサーバー上で実行されるソフトウェアとは別のものです。本来であればサーバーソフトもオープンソースが理想ですが、多くのサーバーアプリは製作者の知的財産権を口実に公開されていません。しかし暗号化は端末で行われるため、サーバーにどの程度の情報が見えているかは、クライアントのソースコードを確認すれば十分です。

4．**アプリを認証する**ためには、アプリのソースコードがオープンにされている以上のものが必要です。つまり、ダウンロードしたアプリが本当にダウンロードされたソースコードに由来していることを検証できる必要があります。これには 2 つのステップが必要です。(1)デバイス上で動作するアプリが、公開された（オープンの）ソースコードから作られるアプリと同一であること、(2)アプリやソースコードが、提供者が公開している真正のものであると確認できること（「自分のアイデンティティを守るために」の章の最後にコンテクストで紹介したような詐欺や中間者攻撃を受けていないこと）です。前者は技術的に難しくて、ユーザーがだれでも検証できるようにはなっていません。しかし、後者は、「暗号化された署名による真正性」の章で説明しているように、暗号署名を使って検証することができます（多くのツールでそうなっています）。

5．アプリは、活発に開発されていて、開発者の反応が良いものでなければなりません。そうでなければ、オペレーティングシステム（Android、iOS など）の変更など、最も基本的なアップデートにも対応できないし、アプリに問題が見つかった場合、アプリのユーザーの情報を安全に保つために、迅速に修正する必要があるのです。

追加の望ましい技術的基準

1．デジタル・セキュリティ・ツールは、**クロスプラットフォーム**が望ましく、広くアクセスできるものがよいのです。「クロスプラットフォーム」とはいろいろな動作環境で、たとえば Linux、Mac、Windows の各 OS や、Android、iOS のスマホで動作することを意味します。また、スクリーンリーダーなどのアクセシビリティに対応したツールであることも重要です。これらの点で安直な妥協はとても問題です。例えば、今はグループ全員が Android 端末を持っているので、Android 専用のコミュニケーションツールを使っても問題ないかもしれません。しかし、将来、Android 端末を持っていない人がグループに参加することになったらどうでしょうか。

2．**セキュリティ監査**とは、能力があり、しかも信頼できる第三者があるツールのコードやサーバーの運用状況を検査して、そのツールのセキュリティを評価することです。ツールによっては、これが無理な期待となってしまうこともあります。例えば、匿名性とセキュリティを重視するため Linux を元に作られた OS である Whonix は、セキュリティ監査を受けていないのですが、実は完全なセキュリティ監査を受けた OS はひとつもありません。

3．**匿名性や仮名性を提供**するツールがより望ましいと言えるでしょう。これは、Tor と互換性があることも意味します。また、仮名のアカウントを簡単に作れるようになっているべきです（登録時に電話番号や電子メールアドレスを必要としない、など）。

4．ツールの**デフォルト**は、ユーザーにとって大きな影響があります。ここ数年、安全なメッセージングが可能なのにデフォルトでは暗号化を有効にしていないアプリを数多く見

てきました。新しい会話を始めるときに、暗号化を有効にし忘れるユーザーはとても多いのです。

5．ツールの**集中化の度合い**によって、サービス品質に影響があるだけでなく、単一のエンティティが管理できるデータ量も変化します。例えば、ある通信アプリがプロバイダーのサーバーを経由してすべての通信を行う場合と、サーバーを使って通信を初期化したあとは、ユーザー間で直接データをやり取りする場合（プロバイダーのサーバーではない他のインターネットの経路を使う）があります。後者はピア・ツー・ピア通信と呼ばれ、ネットワーク内の経路が短縮されて通話品質が向上する、あるいは通話時間などプロバイダに残されるメタデータの量を減らすといったメリットが期待できます。さらに別の選択肢としてフェデレーションの可能性も考慮できます。フェデレーションの例としては電子メールがあり、Google から Microsoft へというように異なる電子メール・プロバイダー間でメールを送信することができます。これに対して Signal では、2 人のユーザーがともに Signal を使用し、Signal のサーバーで通信を確立している場合にのみ通話が可能となります。

技術以外の基準

1．プロバイダが採用した**財務モデル**は、だれがツールへアクセスできるか（アクセス料が必要な場合など）、ツールの長期的な安定性（資金が尽きた場合はどうなるか）、プロバイダの動機（データやメタデータを収益化するのか）に影響を与えます。選択の範囲は、無料、フリーミアム[44]、有料など、多岐にわたります。あるツールが無料で使えるとしたら、その理由を知るべきです。メタデータさえも収益化できる大企業が運営しているのか（Facebook が WhatsApp の連絡先ネットワークにアクセスできるような場合）、それとも寄付や助成金で運営されているのか、調べてください。

2．ツールが[社会]**運動志向**の場合、それはプラスにもマイナスにもなり得ます。「通信を守る」の章の最後で述べたように、運動志向の「May First」によるビデオ会議はサーバー内では暗号化されていないのですが、検閲や当局とのデータ共有を行っていることで知られる「Zoom」よりも信頼できます。一方、VPN では運動系の Riseup を使うとき、使用人口の多い VPN のユーザーの中に隠れるよりも、当局の目を引きやすくなります。

3．事業者の**透明性**は、信頼の構築に役立ちます。「監視と抑圧から身を守る」の章で説明したように、ほとんどの主要企業は透明性レポートを公開しています。多くの場合、これらのレポートは、企業が敵とデータ共有を望んでいることを強調しているに過ぎません。また、「暗号化された署名による真正性」の章で紹介した**令状のカナリア**という方法もあります。

次に学ぶこと

ユーザーの特性や固有の側面について詳細に掘り下げたガイドや参考資料が多数あります。次のリストも利用してさらに検討を進めてください。

Ðigital Ðefenders Partnership. “Ðigital First Aid Kit” https://www.digitaldefenders.org/digital-first-aid-kit . 2021 年 2 月 9 日に確認。

電子フロンティア財団. “Security Education Companion” https://sec.eff.org “. 2021 年 2 月 9 日に確認。

44（訳注）特定のサービスは無料提供し、それ以上のサービスに対してのみ課金するビジネスモデル）

電子フロンティア財団. “Surveillance Self-Ðefense” https://ssd.eff.org/en ” 2021 年 2 月 9 日に確認。

Tactical Technology Collective. “The Holistic Security Manual” https://holistic-security.tacticaltech.org . Holistic Security. 2021 年 2 月 9 日に確認。

Tactical Technology Collective and Frontline Ðefenders. “Ðigital Security Tools and Tactics” https://securityinabox.org . Security in a Box. 2021 年 2 月 9 日に確認。

Powered by PrintFriendly.comPrivacy

Creative Commons License

This work is licensed by Glencora Borradile (© 2021) under a
Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC)

You are free to:
Share -- copy and redistribute the material in any medium or format
Adapt -- remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:
Attribution -- You must give appropriate credit, provide a link to the license, and indicate if
changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
NonCommercial -- You may not use the material for commercial purposes.
No additional restrictions -- You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

クリエイティブ・コモンズ・ライセンス
この作品は、Glencora Borradile (© 2021) により、クリエイティブ・コモンズ 表示-非営利 4.0 国際ライセンス (CC BY-NC) で許諾されています。

あなたは以下のことを自由に行うことができます。
共有 - 媒体や形式を問わず、コピーして再配布することができます。
適応 - 素材をリミックス、変換、および構築すること。

ライセンス条項に従っている限り、ライセンサーはこれらの自由を取り消すことはできません。

以下の条件で。
帰属 - 適切なクレジットを表示し、ライセンスへのリンクを提供し、変更が加えられたかどうかを示さなければなりません。妥当な方法でこれを行うことができますが、使用許諾者があなたやあなたの使用を支持していると示唆するような方法ではありません。
非営利 - あなたは、本素材を営利目的で使用することはできません。
追加的な制限がないこと - あなたは、ライセンスで許可されていることを他者が行うことを法的に制限するような法的条件や技術的手段を適用することはできません。