TF-CSIRT TRANSITS

TRANSITS I

法律モジュール

発表者

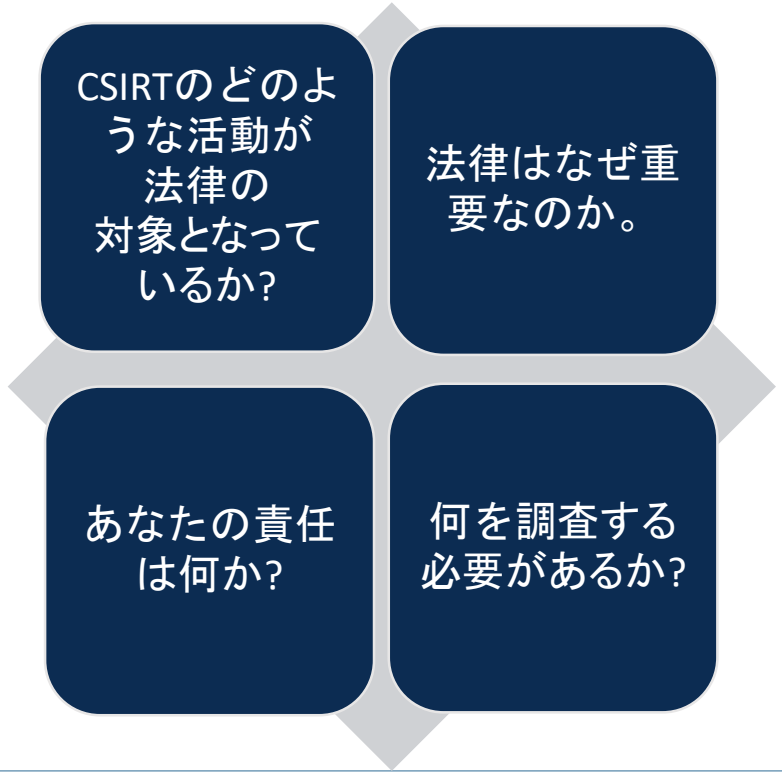
Hamamatsu, JAPAN

11/7/2019

著者:Andrew Cormack、Nicole Harris、Silvio Oertli。

Version:7.0。

学習の目的


CSIRTのどのような活動が法律の対象となっているか?
法律はなぜ重要なのか。
あなたの責任は何か?
何を調査する必要があるか?

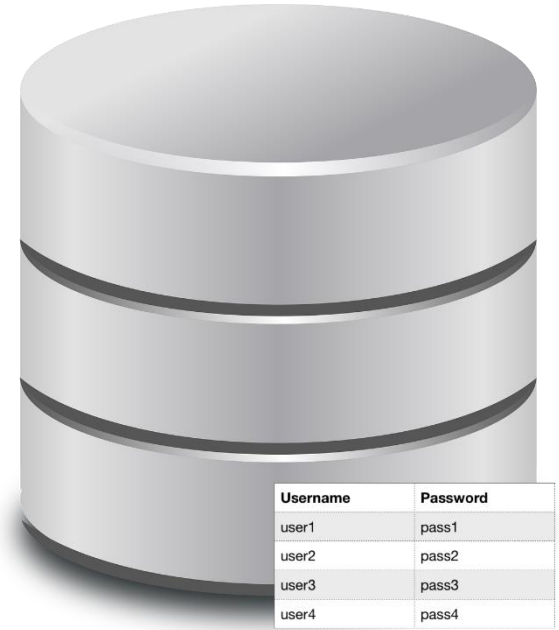
セッションプラン

- はじめに
- 次のような場合に発生する問題。
    1. CSIRTと法
    2. ロギング
    3. コンテンツの表示
    4. 脆弱性のスキャン
    5. テイクダウン要求
    6. 法執行機関との連携
    7. 他の組織との連携
    8. 脆弱性の管理
- 宿題

TF-CSIRT
TRANSITS

Part 1: はじめに

議論1:CSIRTと法律



- ユーザー名/パスワードが設定されたダンプを受領した。
- 「ダークウェブ」内のサイトへのアクセスに使用されてきた。
- ユーザーは自組織と他の組織から成り立っている。
- 警察がコピーを要求してきた。

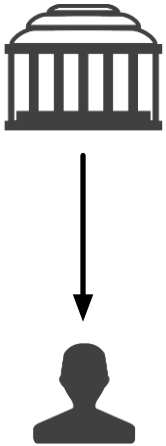
- 何ができるか？すべきことは？しなくてはならないことは？。
- …自組織のCSIRTとしては?
- …組織としては?

TF-CSIRT TRANSITS

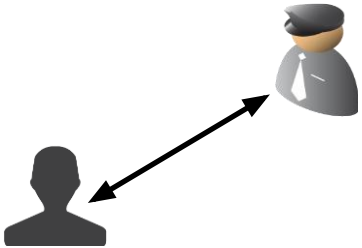
Learnings

- 好き嫌いは別として、法律問題が発生するだろう
- 古い法律、新しい法律、ICT関連法。
- 様々な法域:
  - 公法 → 麻薬、銃器、ハッキングなどの社会的悪事に制限する。
  - 私法 → 他人に与えた損害を修補することがどのように求められるか。
  - 協力 → 警察などの政府機関を支援することを要求もしくは許可されること。

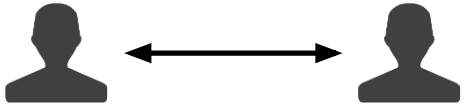
公私法



公法

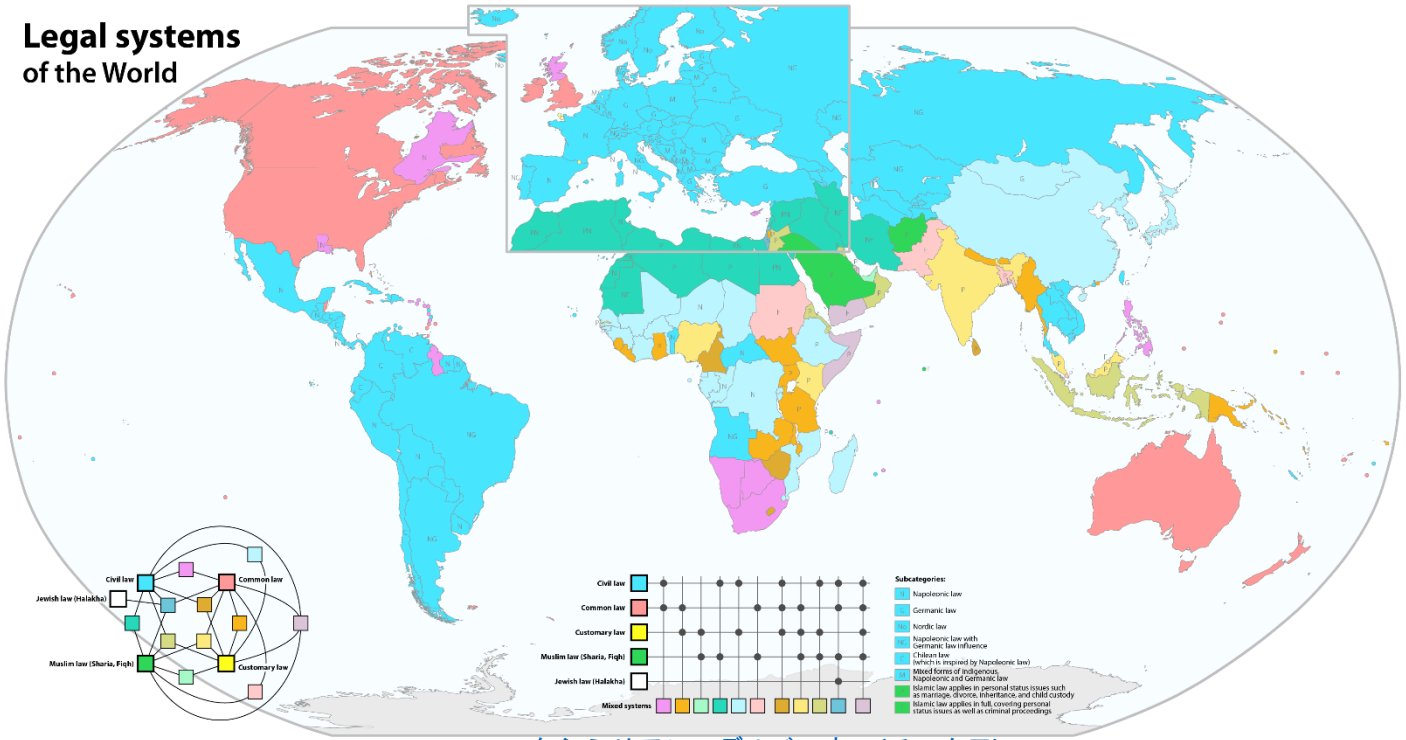


協力



私法

法は国によって異なる



マクシミリアン・デルベッカー(チュムワ)

TF-CSIRT
TRANSITS

Part 2:シナリオ

ディスカッション2:ロギング

- 「悪いやつ」は、あなたが管理するWebメールのユーザーのユーザー名とパスワードを取得した。
- ユーザーは認証情報を使用して、他のローカルユーザーにフィッシング電子メールを送信している。
- 誰が漏えいしたのかを明らかにしたい。

- 調査にはどのようなログが必要か?
- どのような法律問題が発生するか?

ロギング

Learnings

- ログは個人データを含む
- この調査に必要なログのみを使用すること
- プロセスはどのログが必要か教えてくれる
- 保存期間はどれくらいか?

Variability

- EU+一部の国→一般個人情報法(GDPR/Convention108に基づくもの)
- 米国+一部の州→業種特有の法律に基づくもの
  - 健康分野
  - 教職
  - ビデオレンタル
  - 財務

一般データ保護規則(GDPR)

欧州法(2018年以降);　いかなる地域においても影響力がある。

個人データ(Eメール/IP/MACアドレスを含む)のすべての処理に適用される。

明確にインシデント対応を推奨:

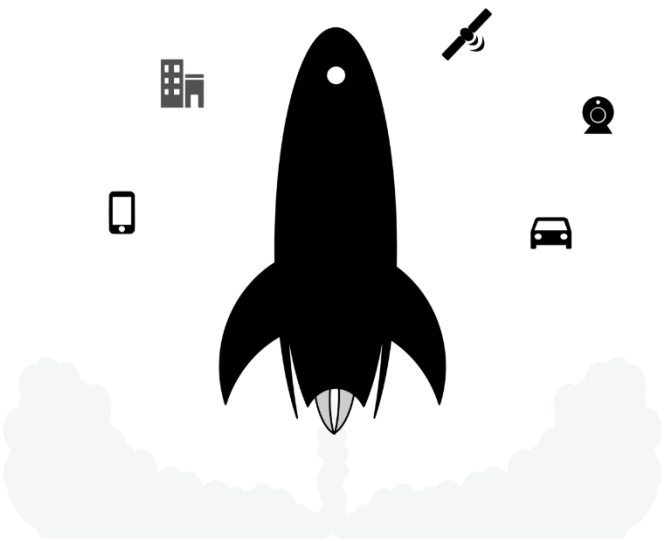
- 侵害通知を通じて、黙示的に要求される。

正当な権利のテスト:

- 目的達成に必要な最小限のデータを処理する。
- 個別のリスクを正当化する、処理のメリット確保する。

キーポイント:　インシデント対応により、ユーザーの個人データとプライバシー関連の保護をより高める。

ディスカッション3:コンテンツの表示



- 携帯電話向けチップに、ファームウェアのアップデートが実装されている。
- このルーチンは、チップベンダーのIPに個人データを送信している。
- データ転送は暗号化されていない。
- あなたは、特定のIPアドレス(シナリオと影響を受けるユーザーの特定)へのトラフィックを傍受している。

- どう考えるか。
- どのよう法律問題が発生するか?

コンテンツの表示

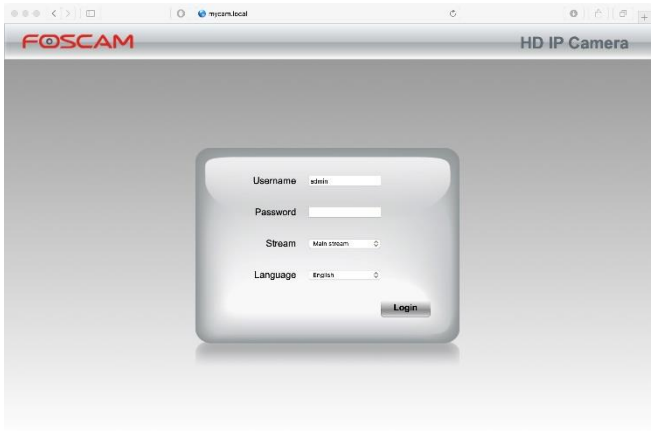
Learnings

- メタデータへのアクセスよりも保護されたコンテンツへのアクセス
- 特定の調査のためだけにコンテンツを検査すること
- 予防対策の実施必要性
- 電気通信に関する特定立法
- 欧州人権条約 (第8条)
  - 私生活及び家庭生活の尊重についての権利

Variability

- 国やネットワークのタイプの間においても高い
- 私益/企業 対 公的/通信

ディスカッション4:脆弱性のスキャン



- 新しいDDoS増幅を発見した。
- CSIRTは脆弱なデバイス/サービスを特定しようとする。
- ログイン画面があった。（ポート80）
- デフォルトのパスワードライブラリを使ってアクセスを試みる

- この行動は合法か?

脆弱性のスキャン

Learnings

- 多くの国には「不正アクセス」法がある。
- 目的/保護/承認/有害性によって異なる場合があります。

Variability

- 高
- その国内から見ても、法律が不明確な場合が多い

ディスカッション5:削除要求（テイクダウン・リクエスト）

- ウェブサイト上で違法コンテンツに関する苦情を受けた場合
- そのウェブサイトは、顧客のサイトにあるようだ
- コンテンツを削除し、再発行されないように要求された

- どうすべきか。
- 日本では、どんなコンテンツが違法なのか。

テイクダウン要求

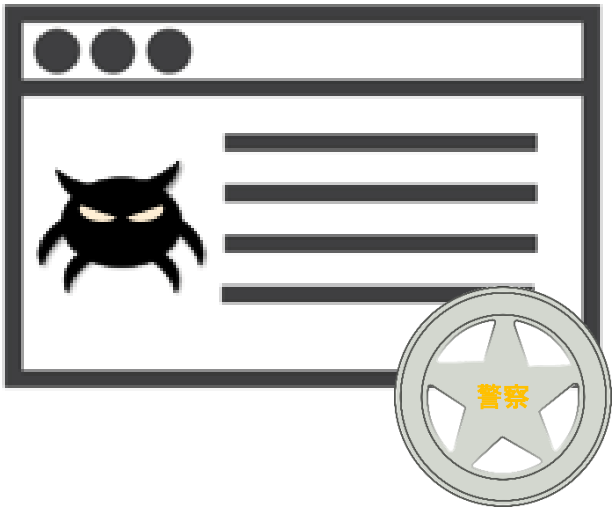
Learning

- 異なる種類の法律がそれぞれ適用される
  - 著作権、ソフトウェアライセンス。テロリズム。ヘイトスピーチ。マイニングマルウェア。マルウェア
- 再発行を防止するための要求はまれであるが、未知ではない
- 発見次第、報告を要するようなタイプのコンテンツの可能性がある。
- 逆に、どこか別の場所にテイクダウンしたいと考えているかもしれない。

Variability

- 高
- 以下の要因による
  - 国
  - コンテンツのタイプ
  - サービスのタイプ

ディスカッション6:法執行機関との連携



- 自社で、クラウドによるインフラを運営している
- サーバが侵入され、マルウェアを配布された
- 警察は、ログ、請求情報の提出を要求
- 警察は、マルウェアの提出を要求

- データを引き渡してもよいか?
- 外国警察の場合何が異なるか?

法執行機関との連携

TF-CSIRT TRANSITS

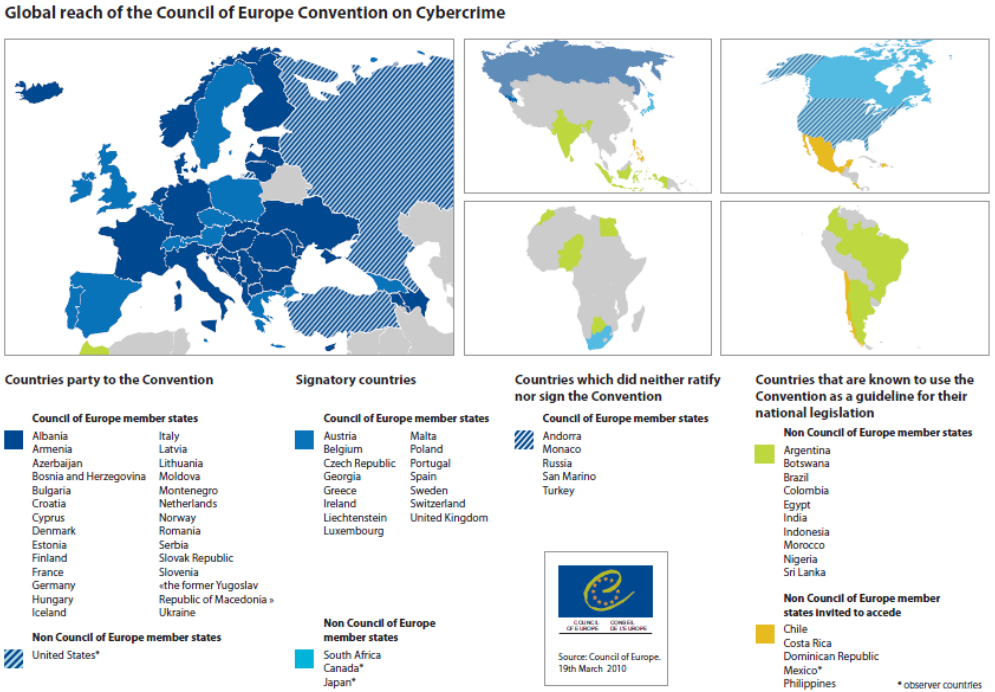
Learning

- 国内法によっては法執行機関への開示を要求/許可/禁止することが可能
- 国際的な情報開示では、さらに次の事項を考慮する必要がある
  - 刑事共助条約
  - サイバー犯罪条約
  - 二国間条約
  - 米国 CLOUD ACT
  - EU E-Evidence 提案
- 警察や各国の弁護士と話す

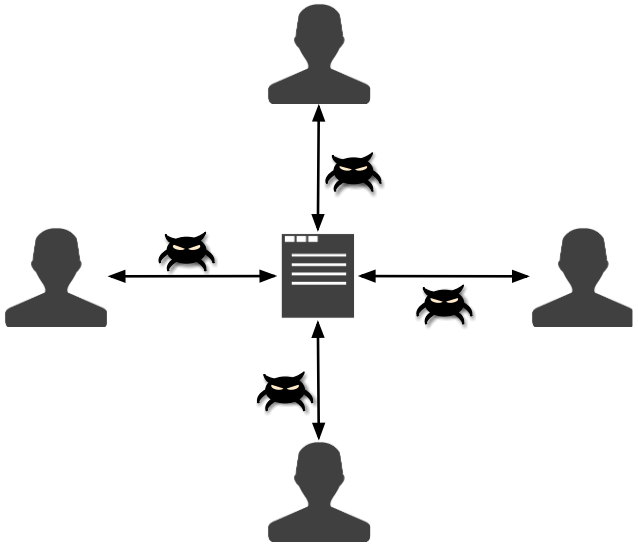
Variability

- 非常に高い
- 以下を基準とする
  - 国
  - 捜査のタイプ
  - コンテンツのタイプ

サイバー犯罪条約(ブダペスト条約)



ディスカッション7: 他の組織との連携



- 新しいマルウェアの一部を解析できた
- マルウェアは電子メールにより流通
- 次の情報を共有したい：
  - 他のCSIRTと、侵入のパターン/インディケーターの共有
  - MISPを通じたマルウェアおよび感染Eメールの共有

- 共有で何が問題になる可能性があるか?
- どうやって回避ができたか?

他の組織との連携

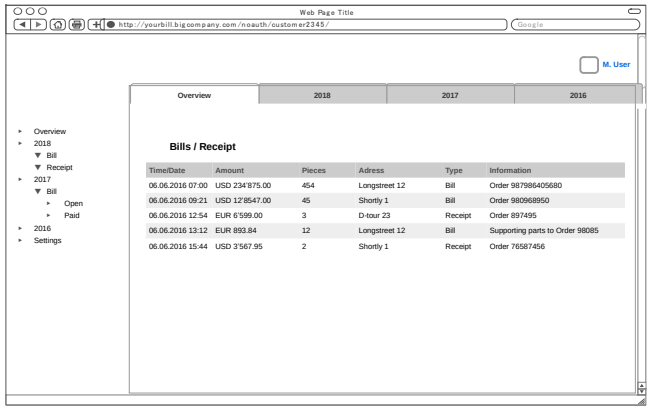
Learning

- 共有のリスクは、それ以上のメリットによって正当化されなければならない
- Traffic Light Protocol(TLP)などの予防措置によるリスクの軽減
- マルウェアを共有することは、「ハッキングツール」の問題が発生する可能性がある

Variability

- データ保護/プライバシーの問題は、比較的、標準のこと
- 「ハッキングツール」の理解は異なる場合がある

ディスカッション8:脆弱性の管理



- 2週間前、自社のWebアプリケーションの脆弱性が報告された
- 組織のメインの電子メールアドレスを使用していた
- 慎重に選ばれたURLの顧客詳細情報にアクセスしていた
- 証拠はスクリーンショット
- 顧問弁護士に送られた電子メールで、警察に通報すると脅している

- どのような法的問題があげられるか?
- どうすれば回避できたか?

脆弱性の管理

Learning

- 研究者は、組織を助けようとしていたようだ
- 法務部の反応としては敵とみなしている
- 脆弱性報告ポリシーを公表すべきだったか
- 未対応の脆弱性によって、データが危険にさらされている個人に対し、責任が生じる可能性がある
- ソフトウェアのリバースエンジニアリングを禁止する法律を含む問題を促進してしまう

Variability

- 調整された脆弱性情報開示についての業績の大部分は、オランダの組織によるもの
- どのような地域でも同じアプローチを適用すべき

TF-CSIRT
TRANSITS

Part 3: 宿題

自組織のどこから始めるか

- 誰が法律アドバイザーであるか、または誰がサポートする担当者なのかを確認しましょう
- CSIRT活動のため、法律を調査し記録しておきましょう。

  例えば...
  - プライバシー/データ保護/モニタリング
  - スキャン/ペンテスティング
  - 通知とテイクダウン（Notice & Takedown)
  - 法執行機関と連携するための社内ルール
  - 情報共有
  - 脆弱性管理/脆弱性情報の開示ポリシー

自組織のどこから始めるか

- 法的通知の認識と取扱の準備
- ポリシーと手順書が、適法に機能しているか確認

Thank you
Any Questions?

著者:Andrew Cormack、Nicole Harris、Silvio Oertli。
Version:7.0。