暗号・情報保全史特論
History of Cryptograph and Signal Security Advanced Course

第8回: 乱数生成・ステガノグラフィ・情報(システム)保全に関する哲学(?)・最近の話題

佐藤永欣

乱数の生成方法

- 周期性のない乱数(疑似乱数でないもの)が暗号には必要
  - （注）状態遷移機械を使って乱数を生成する方法は全て疑似乱数になる
- High-hat法
  - 袋etcに入れた数字を書いたカードを無作為に取り出す
    1. 4桁または5桁の数字を書いたカードを1000枚または10000枚用意する
    2. 袋に入れてよくかき混ぜる(箱だと端っこの方がなかなか混ざらないとかいろいろノウハウがあるらしい)
    3. 1枚だけカードを取り出す→乱数表に載せる
    4. カードを戻して2に戻る
  - High-hat: 山高帽
  - 原始的だが確実なので電子計算機が暗号通信に利用されるまで使われた
- その他に10面体のサイコロ、ルーレットなども使われた

乱数の生成方法

- 組み合わせ乱数
  - 厳密には疑似乱数: 周期が発生し得る
- ホルトン-スミス法
  - 部隊が孤立する→乱数が足らなくなる→でも新しい乱数表を届けられない
  - 既存の乱数表から新しい乱数表を間に合わせで作る
    - 送受信双方で旧乱数表の開始位置ページ・行・列を2か所(a,bとする)をどうにかして共有
    - c=a+b (mod n)またはc=a⊕bを計算。Nは乱数表の桁数による。海軍は5桁なので100000。⊕はここでは桁上りを無視する加算
    - 旧乱数表でaとbの位置を1ずつずらしながらcを生成し、新乱数表に使う
    - 厳密には周期性が出るがaとbを変えれば乱数表の大幅な水増しができる
    - aとbの共有には真の使い捨て乱数を使った通信をしたり決死隊の航空機を送ったり
  - ラバウル方面は昭和18年夏以降孤立
  - この方法で耐えしのいだらしい→「孤立部隊の通信を狙え」と米軍が暗号解読者を集中投入したが解読できなかった

乱数の生成方法(疑似乱数; おまけ)

- (線形)合同法
  - 意外と新しく1949年考案(レーマー)
- 平均採中法(二乗中抜き法)
  - これも意外と新しい(フォン・ノイマン)。元の文献がないが1946年から1949年といわれている(KnuthのThe Art of Computer Programing等による)

  1. 2n桁の数字aを適当に思いつく
  2. a^2を計算→4n桁の数字ができるので中央の2n桁を取り出して次のaにする

- 合成法(これも結構新しい。原典はよくわからなかった)
  - 長さが異なる適当な数列a_1～a_nを作ってそれぞれ1行にくりかえし並べる
  - 縦に足して乱数にする(桁上りは無視)

a_1	1	2	1	1	2	1	1	2	1	1
a_2	0	2	2	1	0	2	2	1	0	2
a_3	3	4	5	7	4	3	4	5	7	4
a_4	2	1	2	3	9	5	0	2	1	2
計	6	9	0	2	5	1	7	0	9	9

乱数表に対する保安

- 陸軍の完全使い捨ての乱数表(海軍では特別乱数・特乱と呼んだ)
  - 陸軍は戦略レベルの暗号に完全に使い捨ての乱数を使用していた
    - 米軍でいうトイレットペーパー
- 陸軍の乱数表の構成
  - 冊子体に製本した乱数表が配布される
  - ページの片面に乱数表が印刷されている。裏側は真っ黒に印刷
  - 乱数表の数字側の面は袋とじのようになっていて黒い紙が貼ってあった
  - 乱数表の使用開始直前に黒い紙をはがした
  - 使用開始前に盗み見られることもない
    - 大使館などの駐在武官も持っていた→清掃作業などには現地で人を雇うし泥棒も入る→スパイかも?
    - 暗号書を写真撮影して情報を盗むのは常套手段だった(昔のカメラは大きかったが)
      - 写真撮影のために黒い紙をはがすとバレてしまう

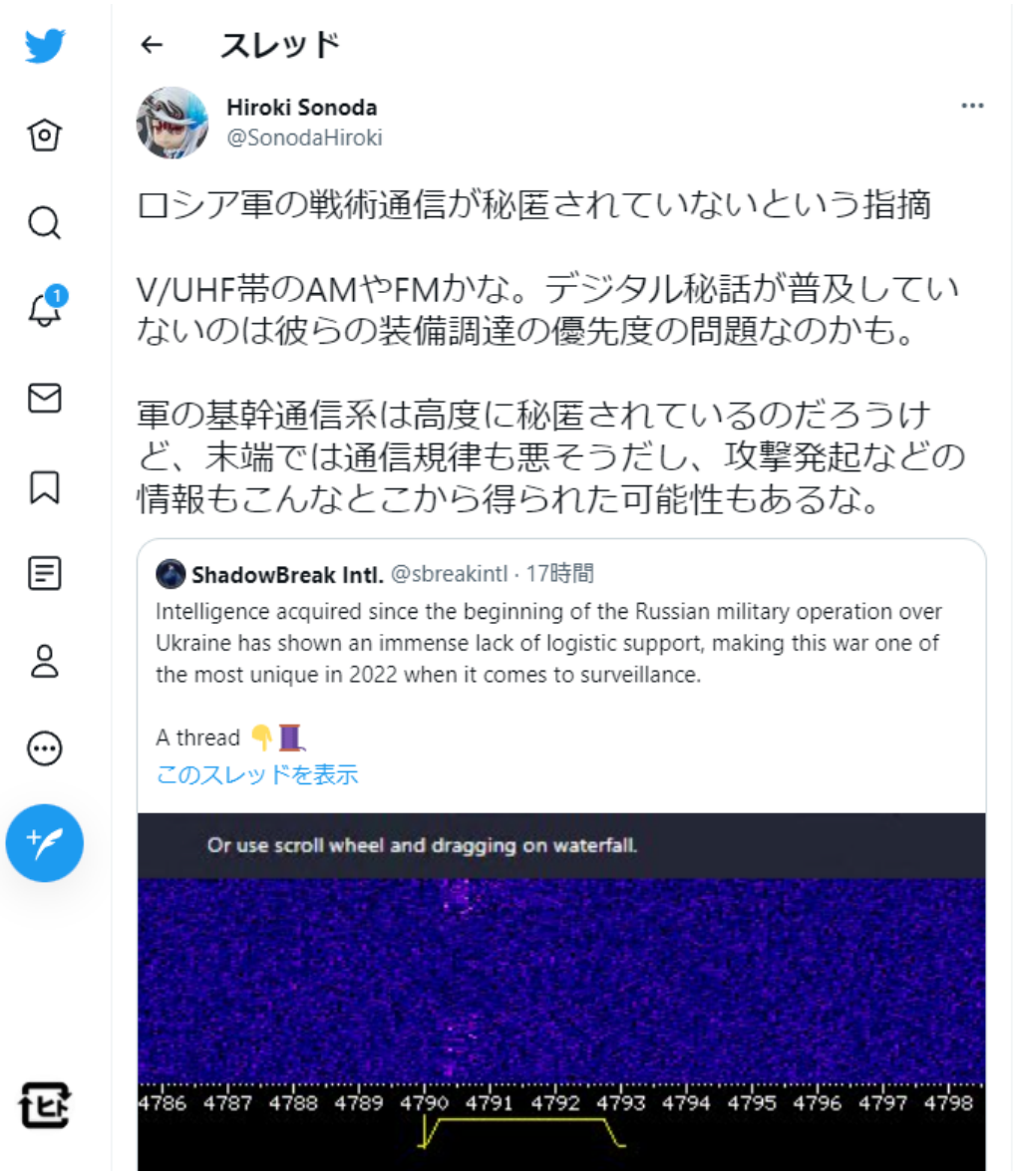
通信の保安全般について

- 暗号強度が違う通信が入り混じる
- 通信文自体は違っていても、組織として同じ目標に向かっている以上、通信文の内容は全て何らかの関係がある
- 例)
  - 上級司令部からの作戦命令: 〇月×日払暁をもって△地点に攻撃を開始し占領せよ。近接航空支援もあるので空軍の□□飛行隊と連携せよ
  - 作戦命令を受けた部隊が考えて実行すること
    - あ～、弾薬準備しないとな～。各車両に積めるだけ積んでおかないと
    - おっと、食いもんと燃料もいるぞ。調理はやってられないから携行糧食に切り替えだ
    - 寝る場所がいるから今のテントは撤収だ
    - 補給部隊と攻撃開始後の補給の段取りもつけなきゃ
    - 近接航空支援で飛んでくる飛行機との通信方法の準備をしなきゃ
  - これに関する通信が大量に行われることになる→大量なのが重要!!!!!!

2022年の例1

https://twitter.com/SonodaHiroki/status/1498651291144183815

- ロシア軍の基幹系の通信は暗号化されている
  - さすがに近代化された正規軍なので?
  - おそらく現代暗号なので計算量的に安全
  - 普通の軍はデジタル化した音声を暗号化
- 末端がダメダメなんてもんじゃなかった
  - 4MHz帯のHFのSSB無線を秘話なしで使用
  - さらに末端は30～50MHz程度のVHF無線
    - FMかAMかSSBかはわからない
  - アマチュア無線機とアンテナを持ってればだれでも受信できる
    - 10万円～
  - 中華製のHFを受信できるラジオでも可
    - 2万円～。DSPラジオですごくいいのがある
  - しかも情報秘匿に対する規律が緩い
- で、どうなったか?



https://twitter.com/SonodaHiroki/status/1498858463086010370

2022年の例1

- 一般の装甲車両のアンテナはこんな感じ
  - アンテナの長さで通信に使っている周波数を推定できる
    - 基本は5/8λか1/4λ。
    - 2mぐらいなのでVHF帯。50MHzよりは下?
    - HFアンテナはもっと長くなるか、アンテナの途中にコイルを挿入して短くする
- 電波の周波数によって通信できる範囲が変わる
  - 携帯電話でもあるよね? 800MHzは田舎に行くと必須とか
  - 周波数が低い方が広範囲で通信しやすい
  - しかし帯域幅が狭い→デジタル秘話装置を作りにくい

https://twitter.com/SonodaHiroki/status/1498651291144183815

2022年の例1

- 末端の戦術レベルの通信内容から上部からの命令が推測できる
  - 部隊給食から携行糧食への切り替え指示
  - 弾薬引き渡し
  - 燃料引き渡し･補充
- この手の情報を広い範囲で集めて総合すると、何日ごろ何が起きるかを推測できる
  - その結果戦術的奇襲にも失敗した

2022年の例1

- これ、本当??というような情報
  - https://defence-blog.com/russian-soldiers-uses-chinese-portable-radios-during-kremlins-invasion-of-ukraine/
  - BaoFeng UV-82HP
    - 144MHzと430MHz
    - アマチュア無線機なので秘話機能なし
    - 出力5W、付属のポータブルアンテナでも10～20kmぐらいは通信できるか?
  - Amazonで70ドルぐらいで買える
    - https://www.amazon.com/dp/B00Z52HP10
  - どこから突っ込んでいいのかわからん
- ウクライナ側は最新の戦術用無線機を使っている模様
  - Harris, Motorola, Aselsan製
  - デジタル秘話付き
  - スペクトラム拡散されているだろうから、帯域幅あたりの送信電力が小さい→発信源を探知しにくい

Sunday, March 20, 2022

DEFENCE BLOG

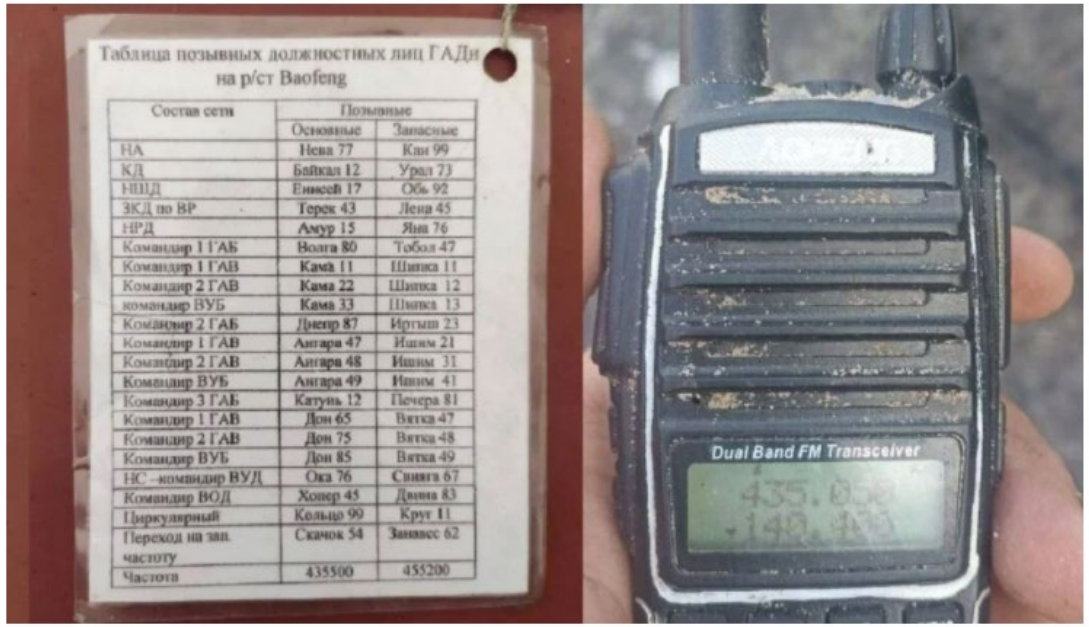
HOME NEWS TRENDING NEWS ANALYSIS INTERVIEW PHOTO VIDEO ABOUT US

LATEST NEWS Russia uses western components for its combat vehicles

Russian soldiers uses Chinese portable radios during Kremlin's invasion of Ukraine

NEWS ARMY By Dylan Malyasov | Mar 13, 2022

Modified date: 5 days ago



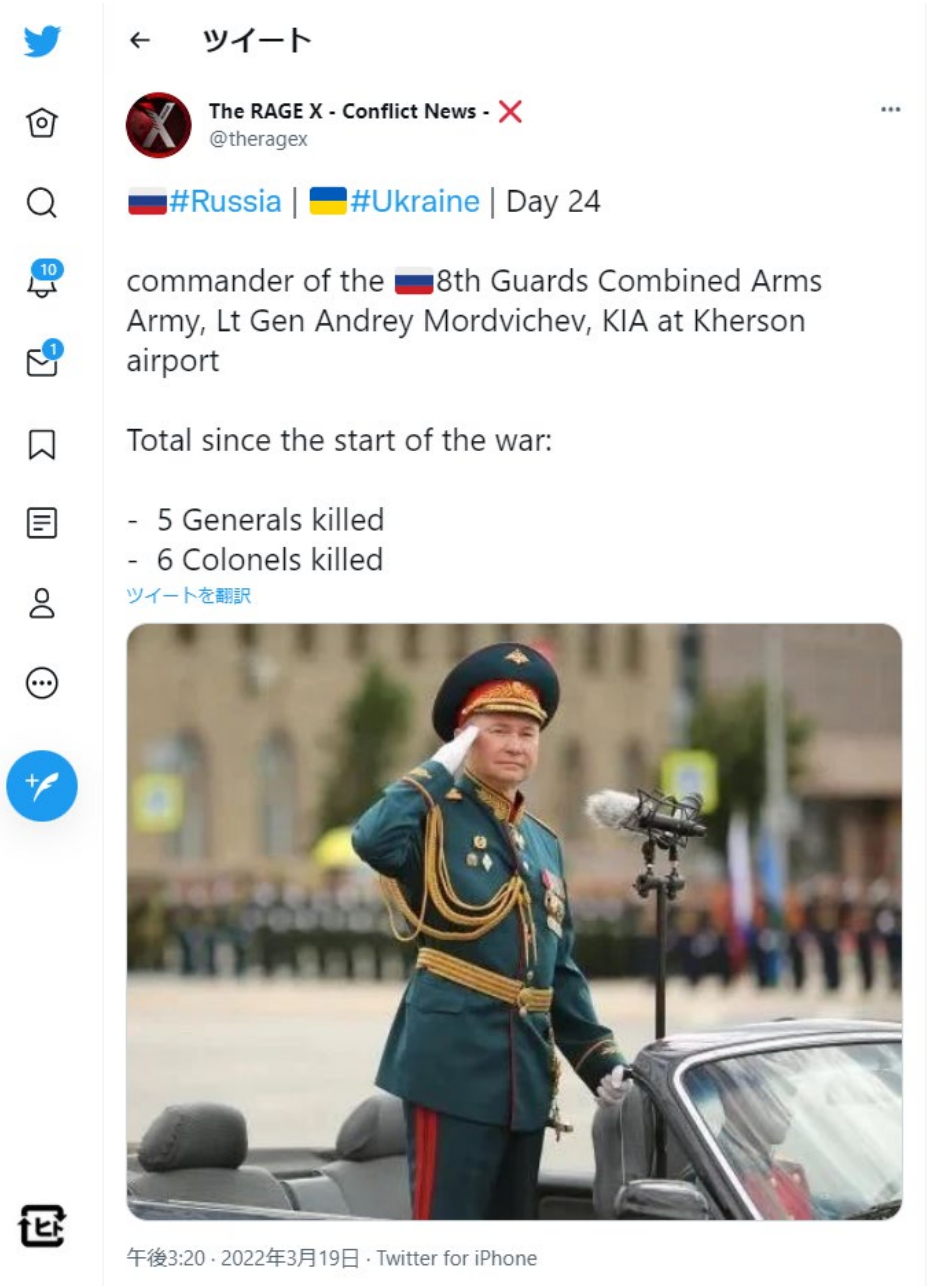
The Russian military has used civilian mobile phones and radios for their communications, including Chinese-made civilian handheld radio, during the ongoing Kremlin's invasion of Ukraine.

According to the Defense Express magazine, the Russian military is using the BaoFeng UV-82HP radios for communication within the frontline units currently stationed in Ukraine.

https://twitter.com/theragex/status/1505066737724760064

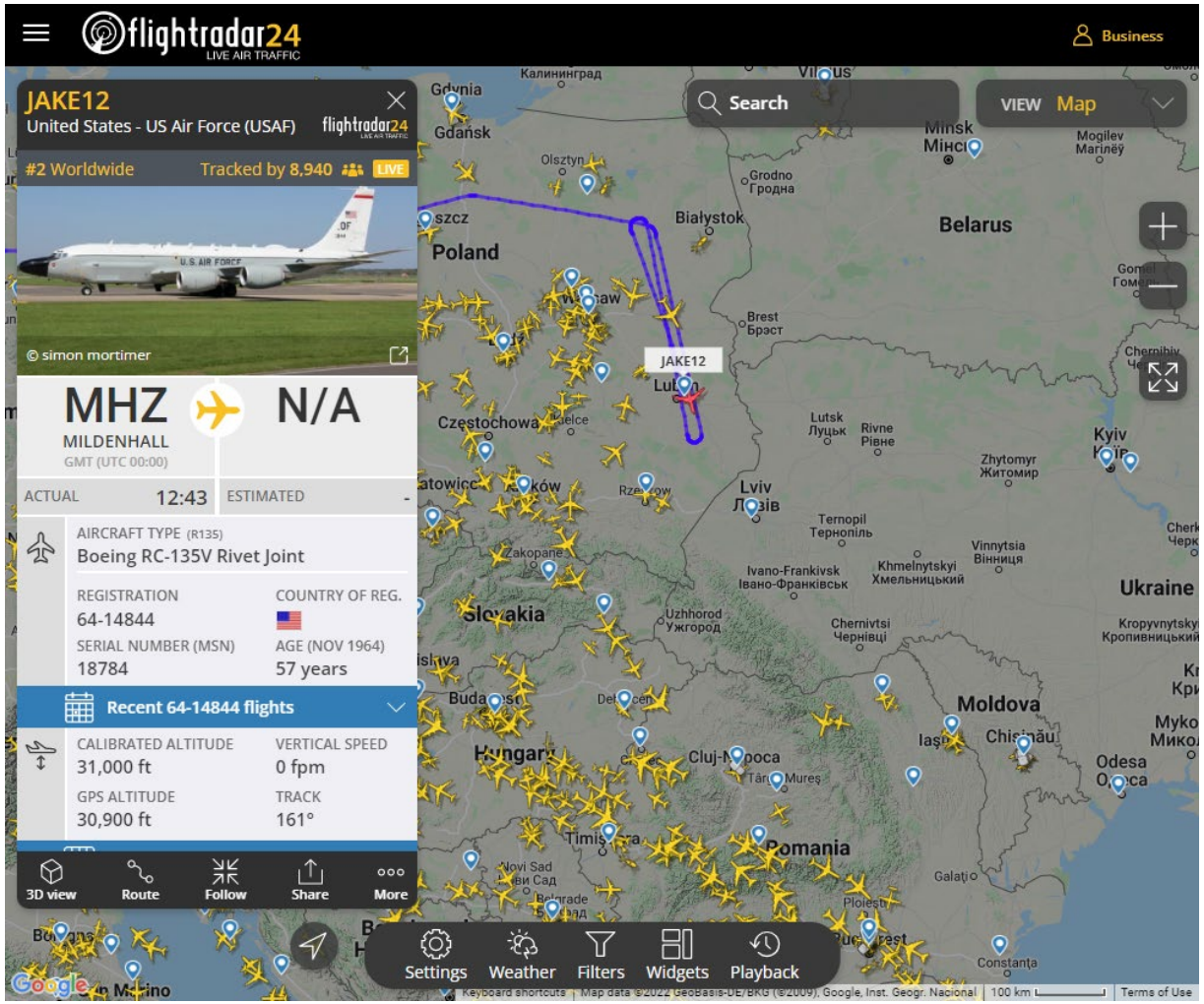
2022年の例2

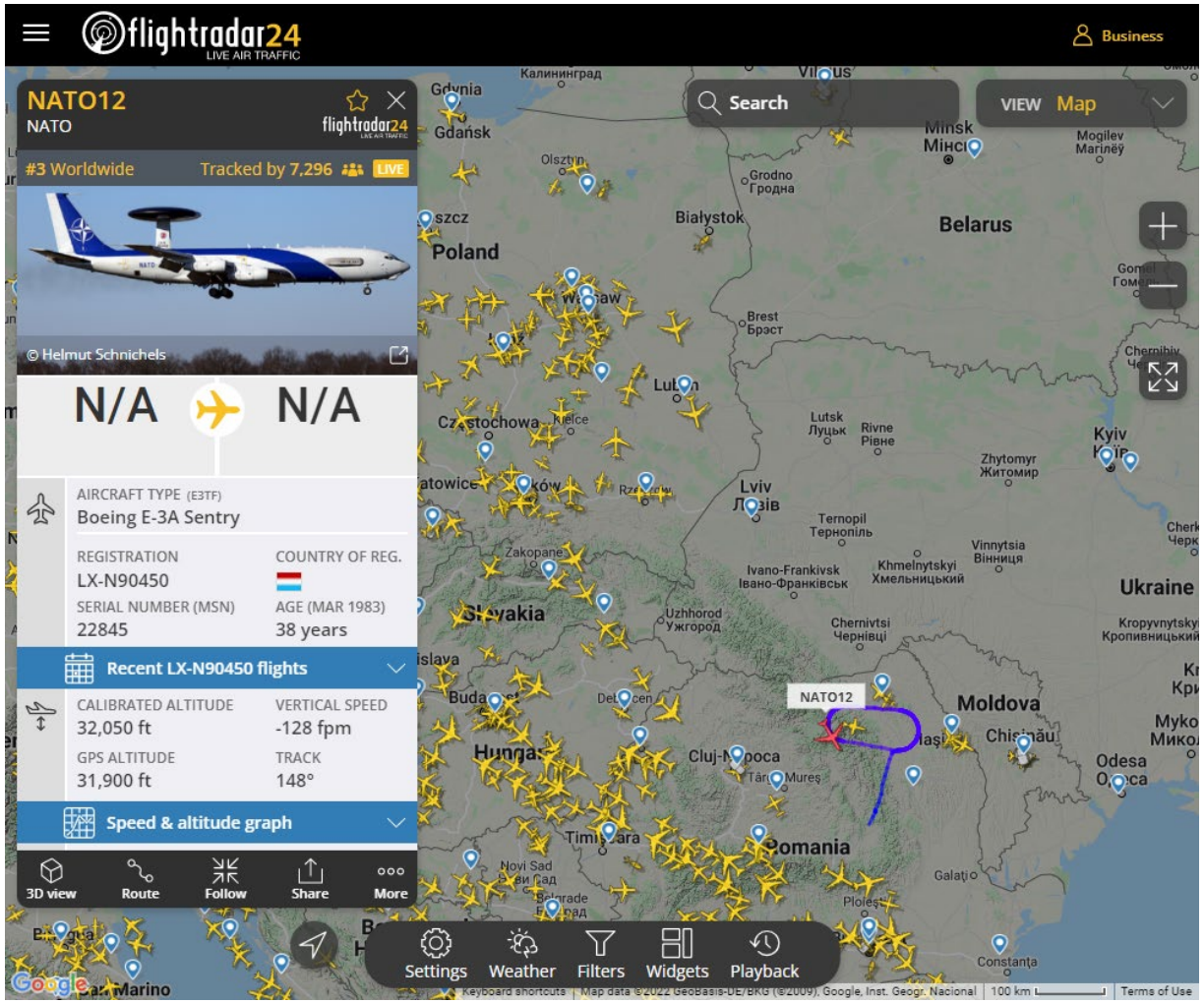
- 開戦24日目
  - 少将・中将5人戦死(31日目の3/26に7人目追加)
    - ブチ切れた部下に戦車で轢かれて死んだのもいるが
    - 軍団長・師団長・副師団長・旅団長
    - ウクライナにいるロシアの将軍は編成上20人ちょいぐらいのはずなので、前線の兵より損耗率が高い
      - 前線の兵で最大で10%程度という見積り
  - 大佐6人戦死
    - 旅団長・連隊長
- 今までの常識では「偉い人」はまず戦死しない
  - 弾が飛んで来たり気軽に撃てる携帯ミサイルが飛んでくるようなところにはいない
    - 司令部にそんなものが飛んで来たら負け確定。数時間以内に戦闘不能部隊続出になるレベル
  - 日本陸軍の例で言うと、玉砕レベルでないと戦死しない
  - が、司令部だけが攻撃されて司令官+幕僚が戦死するパターンが異常に多い
- なぜだ!!!!!!!!!!!???????????



2022年の例2

2022年3月24日15:43 UTCごろ
なにやら怪しい飛行機がうろうろしているぞ?

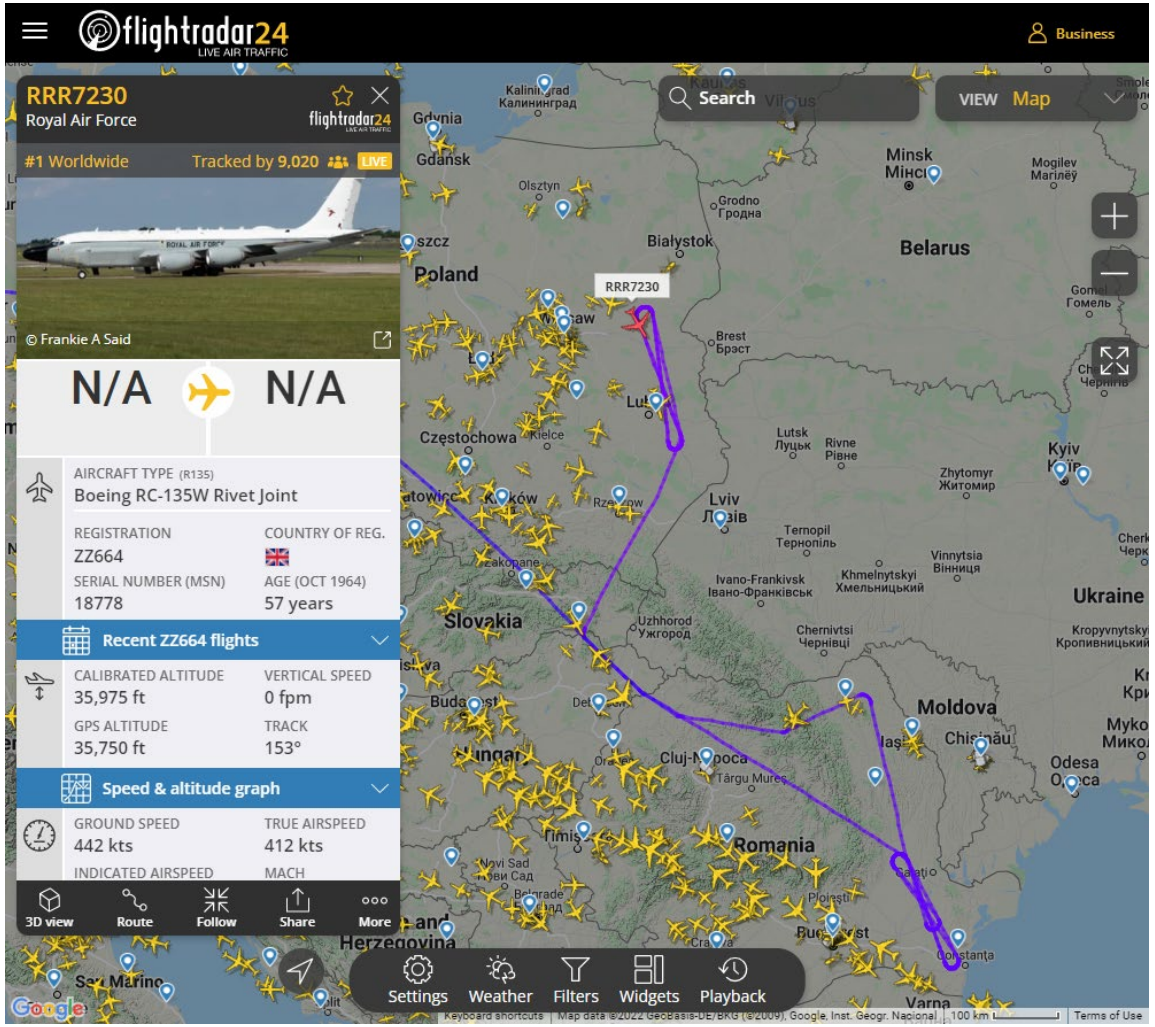




2022年の例2

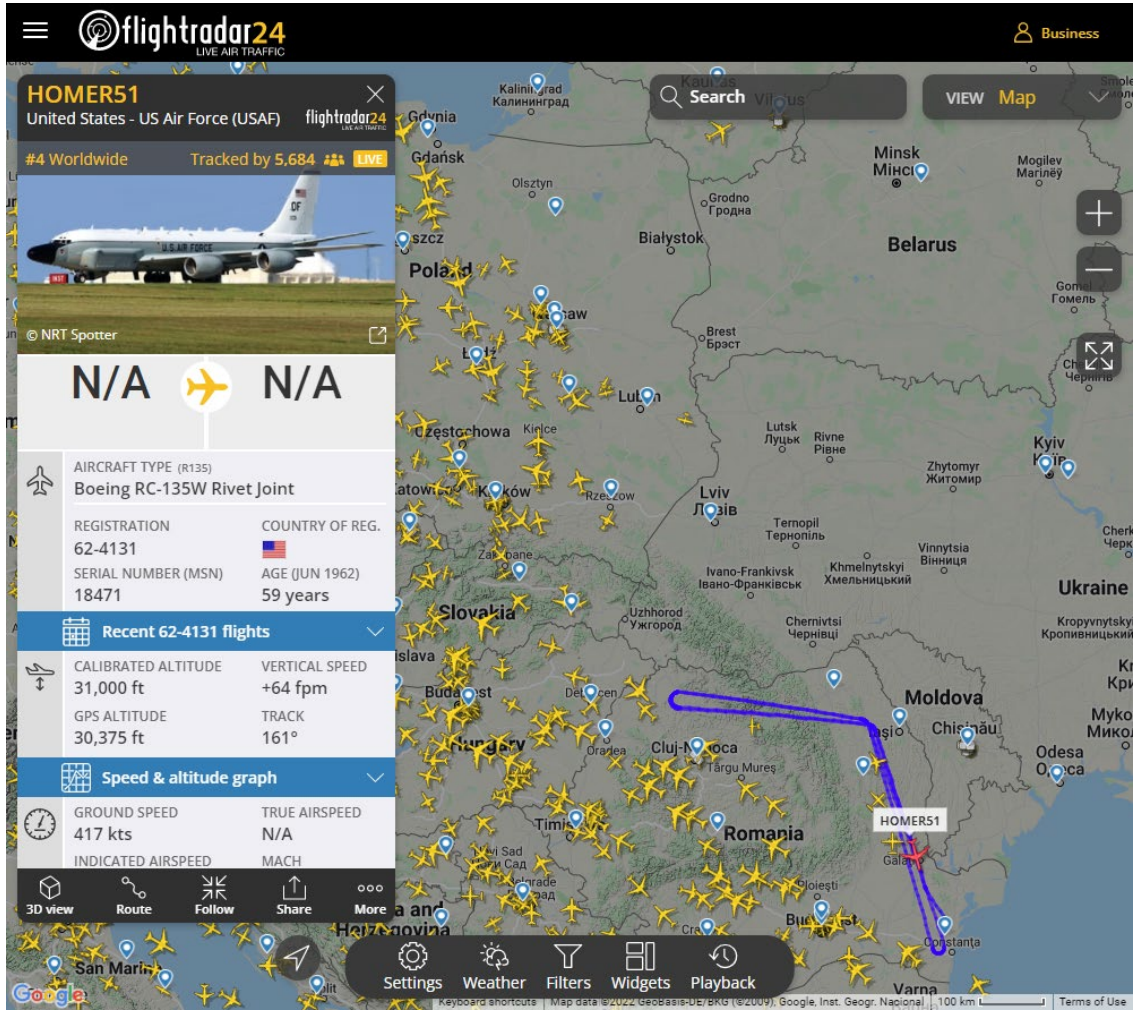
2022年3月24日15:43 UTCごろ
なにやら怪しい飛行機がうろうろしているぞ?

- アメリカ空軍のRC-135V
- NATO各国軍共有のE-3C (ルクセンブルグ登録)
- イギリス空軍のRC-135W
- 飛んでいるのは昼だけ
  - 何をしているか推定するには重要
    - 昼夜で電離層の状態が変わる
    - 短波(HF)でも低い周波数は夜間の電離層反射が強くなる
    - 4MHzあたりらしいので、夜間は電離層反射波が強い。昼ならごく弱い
      - 夜に遠くのAM(中波)ラジオが聞こえるのと同じ理由
  - 開戦前～直後は24時間飛んでいたような?



2022年の例2

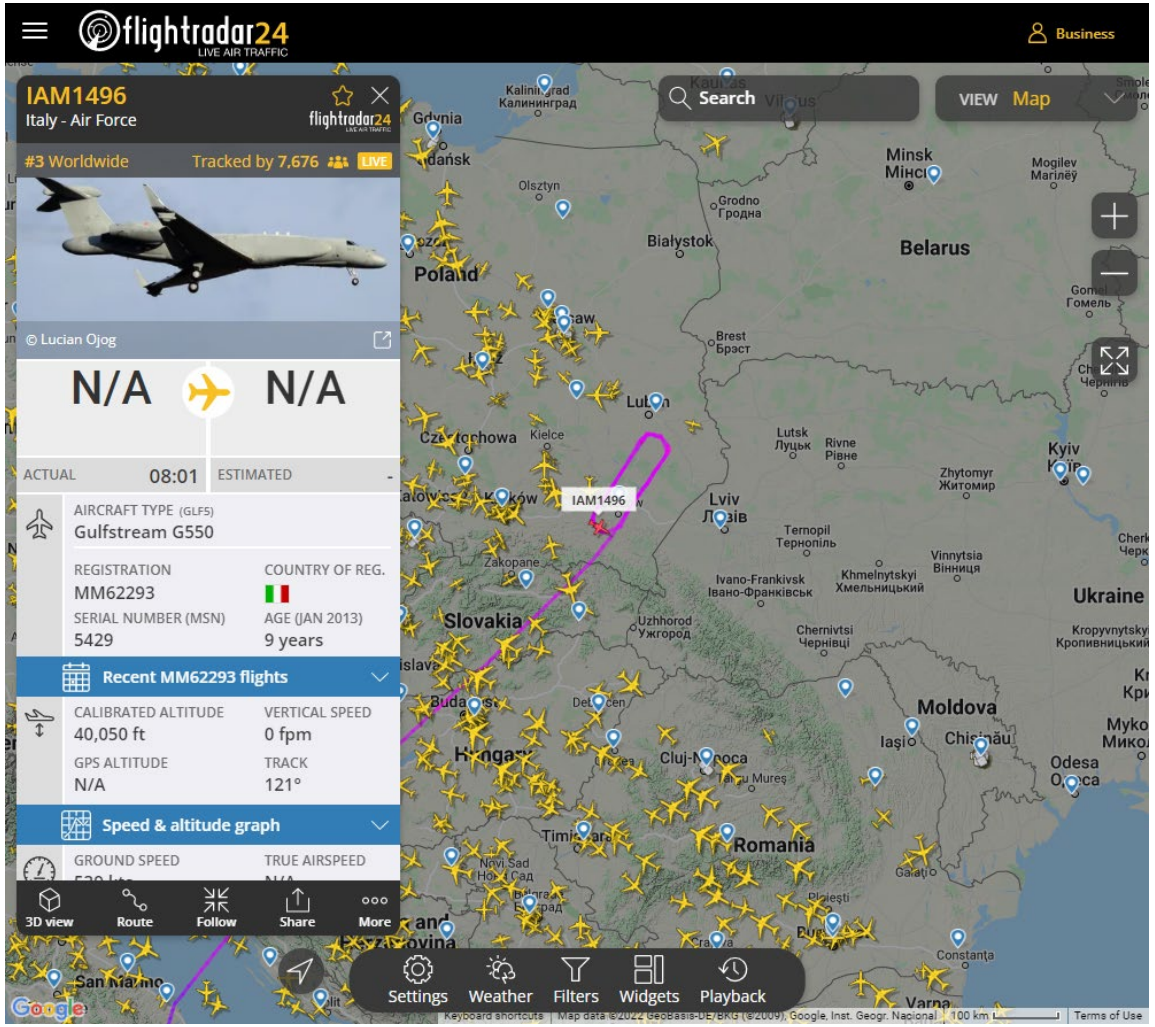
2022年3月25日10:25 UTCごろ
なにやら怪しい飛行機がうろうろしているぞ?



2022年の例2

2022年3月25日10:25 UTCごろ
なにやら怪しい飛行機がうろうろしているぞ?

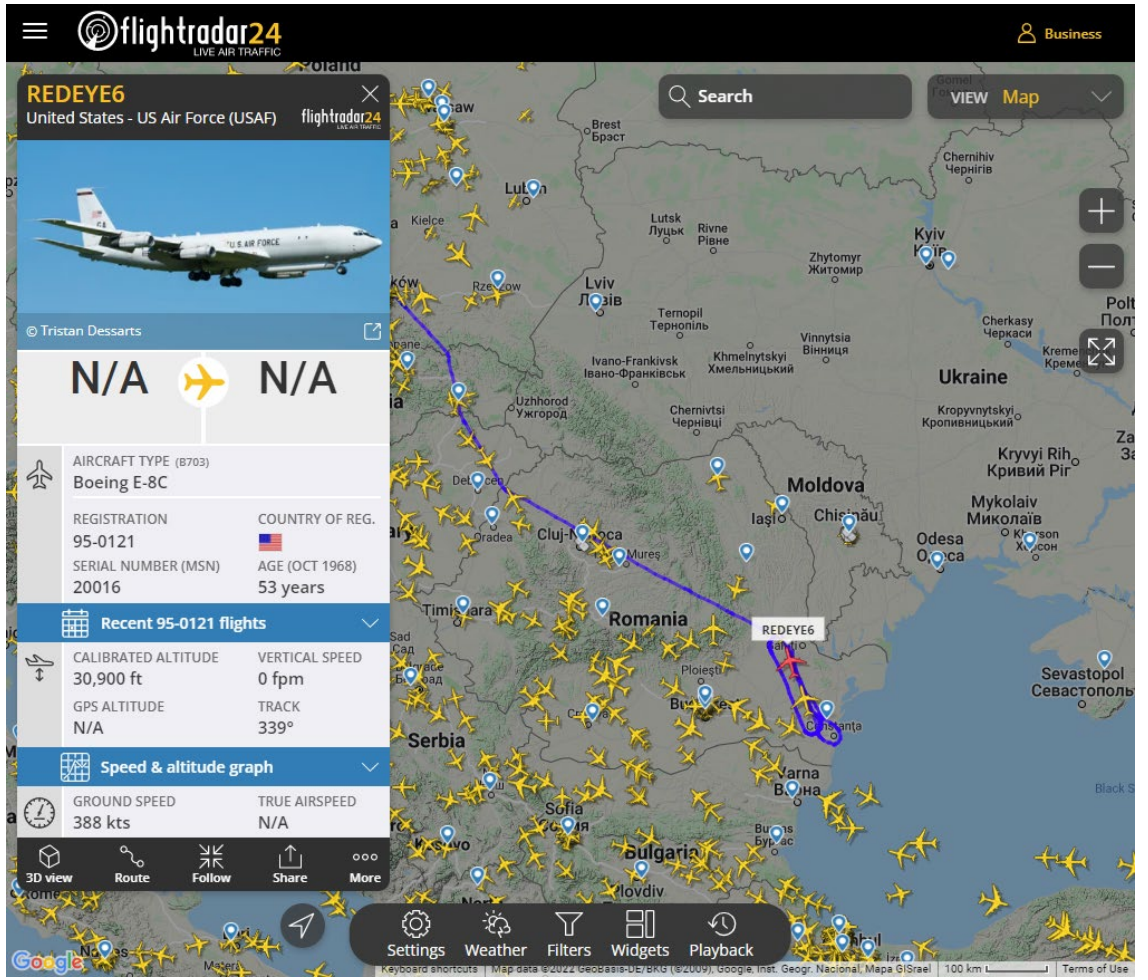
- アメリカ空軍のRC-135W
- スウェーデン空軍のガルフストリームII改造機
  - S102B Korpenらしい
- イタリア空軍のガルフストリームG550改造機



2022年の例2

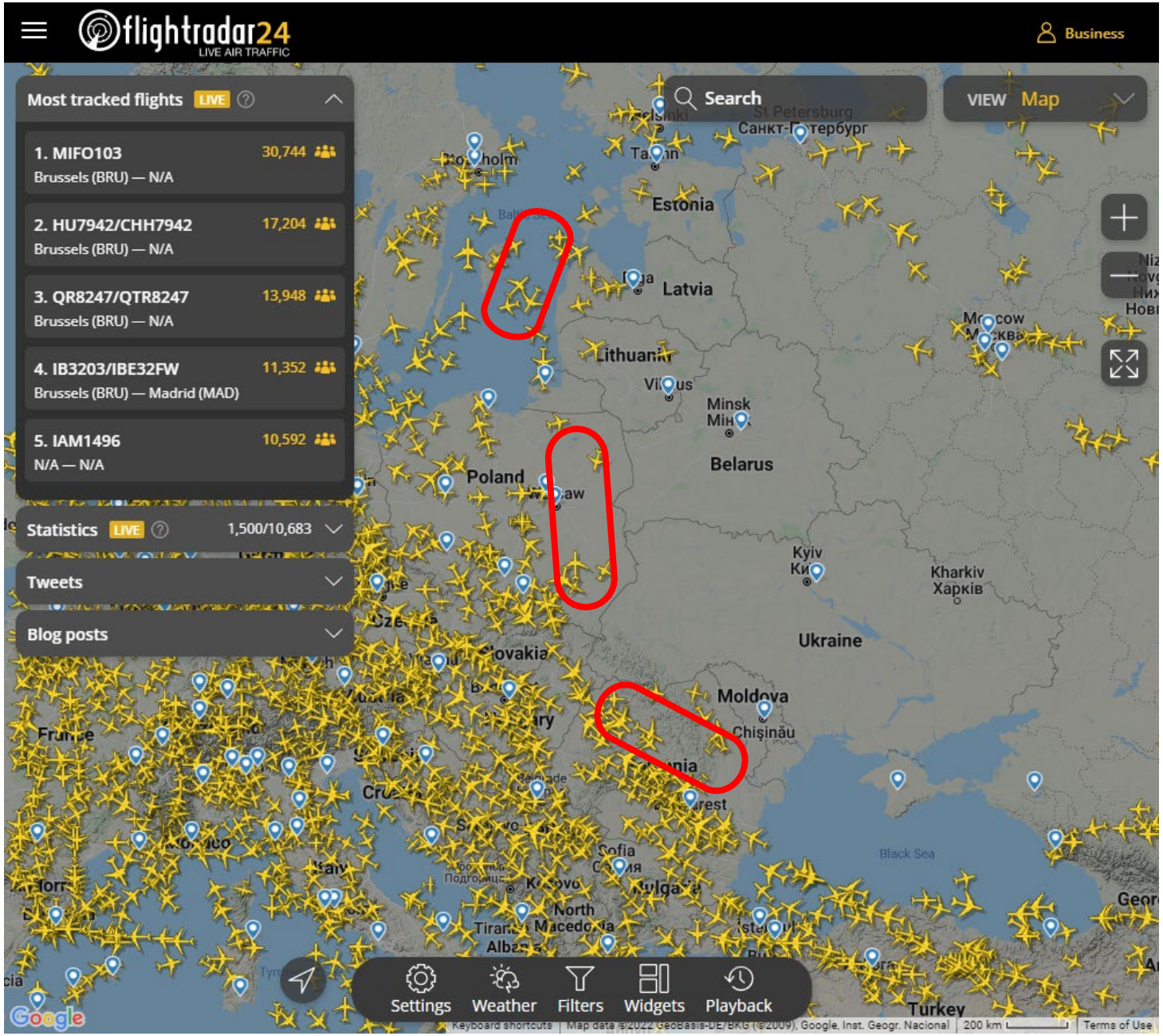
2022年3月25日12:42 UTCごろ
なにやら怪しい飛行機がうろうろしているぞ?

- 前ページの3機にE-8Cが加わった
  - ちょうどこのタイミングでバイデンか閣僚が乗ったアメリカのC-32AがRzeszow (ポーランド南東部)に到着したので警戒態勢強化???



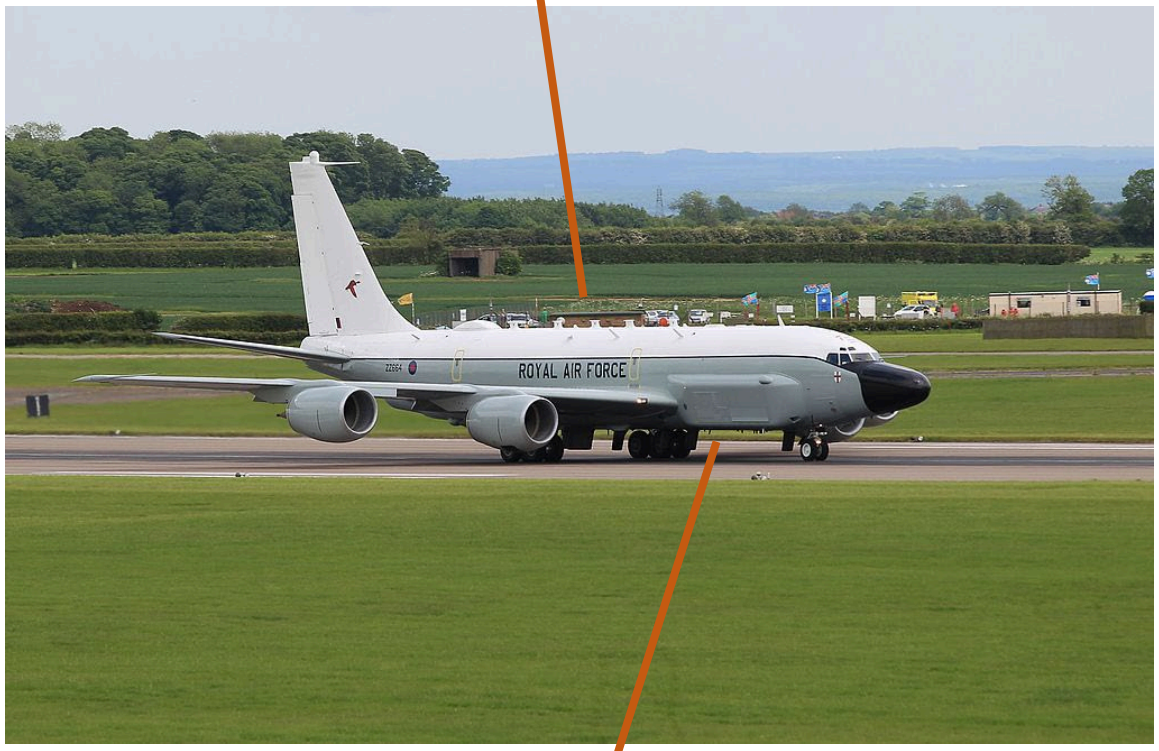
2022年の例2

- 電子戦偵察機・早期警戒管制機が、同時に何機も違う場所で旋回していた
  - 場所
    - ポーランド東部国境
    - ルーマニア北東部国境
    - バルト海
  - 機種
    - RC-135U/V/W(米・英空軍)
    - E-8C(米空軍)
    - E-3A(NATO共有)
    - EP-3E(米海軍)
    - Challenger 60(ルーマニア, アメリカ登録説あり, N488CR他)
    - ガルフストリームIV改造 S102 Korpen (スウェーデン空軍)
    - ガルフストリームG550改造機(イタリア空軍)
- これが何をしていたか?



2022年の例2

- RC-135U/V/Wの能力
  - 長距離の電波受信能力
    - HF、VHF、UHF
    - VHFとUHFは見通せる場所なら電波が届きやすいが陰に隠れると弱い
      - 周波数が高いほど電波の直進性が高い
      - 建物の陰で圏外になったりしたよね?
- 上空を飛んでいるので遠くまで見通せる
  - ほぼ3万フィート以上: 9000m以上
  - 概ね400～500km見通せる
- つまり、直接波で発信源から偵察機に電波が届く
  - 反射したり回折したりしない
- 弾道ミサイル発射監視用RC-135S/Xとは能力が違う



見えにくいがVHF/UHF
アンテナが機体の上下に
大量に生えている

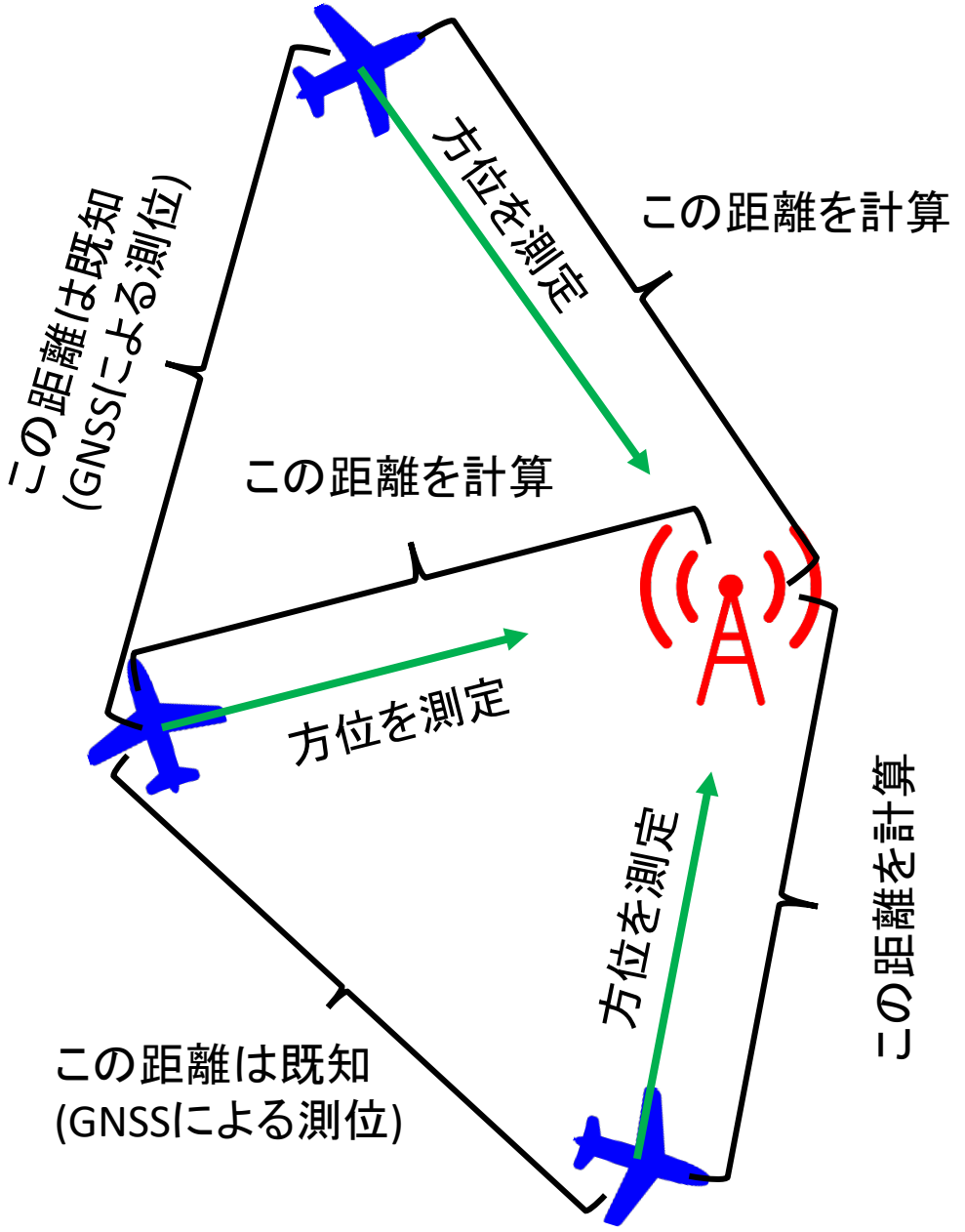
アンテナを収容するフェアリング
HF電波を受信するための大きなアンテナが
入っているとされている

2022年の例2

- E-3セントリー(AWACS)の能力
  - レーダー電波発射
  - 航空機の位置管制
  - 指揮管制/広域監視/戦場管理
- やはり電波がどの方向から飛んでくるかはわかる
  - ポーランド-ウクライナ国境、ルーマニア-ウクライナ国境付近から概ねドニエプル川の西側は完全に監視できるとされている

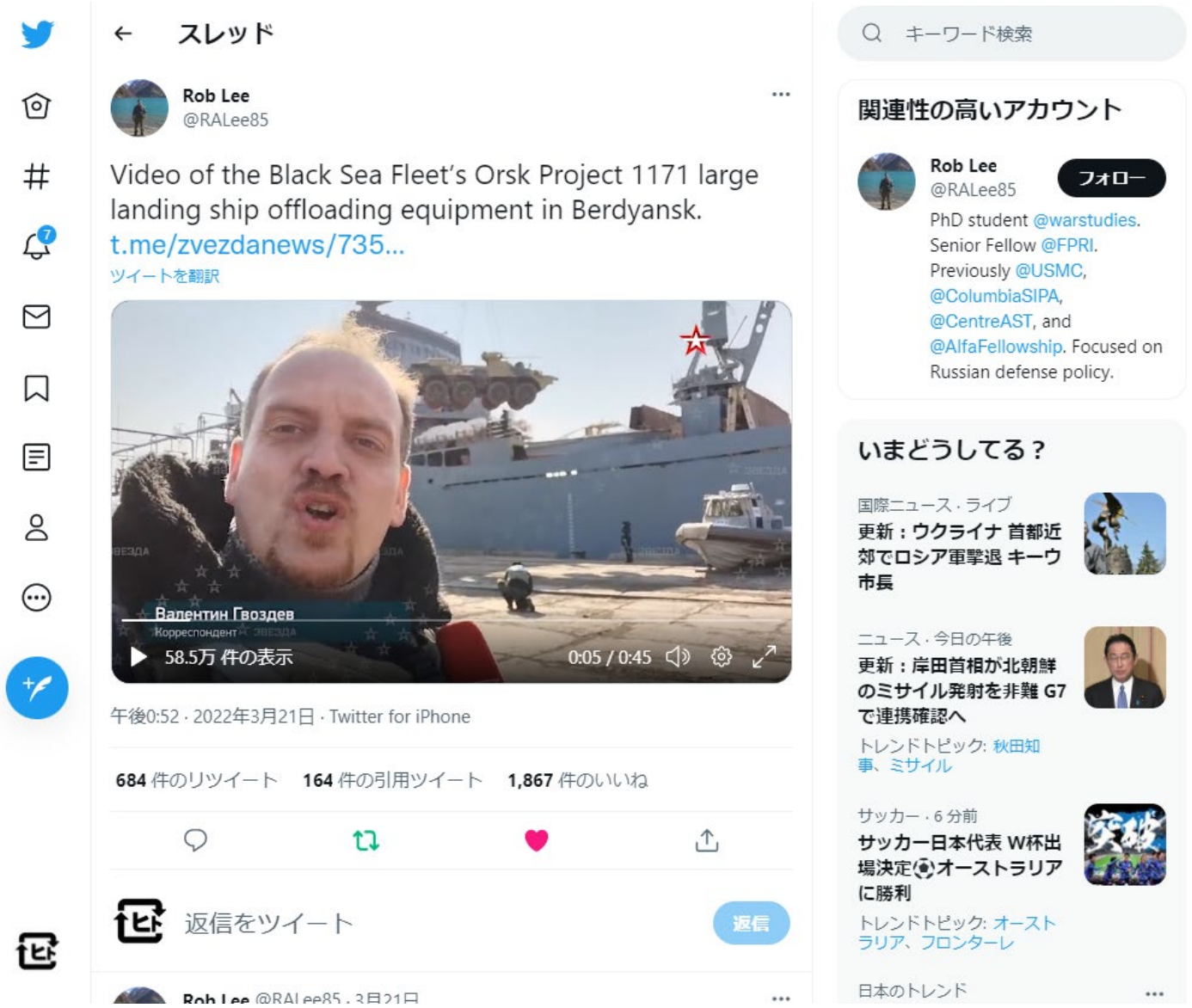
2022年の例2

- ここからは想像でしかない
  - 同時に2カ所以上から電波が飛んでくる方向を確定
  - あとは三角測量すれば電波の発射源は特定できる
  - 偵察機の時計を正確に合わせておいて、電波の位相差から距離の差をもとめる方法もある
- 司令部は通信量が多い
  - 配下の部隊とのやり取りetc
  - 規模もあるので移動させるのが大変
    - 数十人～百数十人程度分の敷地＋テント
- 電波の発射回数が多いところをマッピング
- マッピングされた場所を攻撃してみる
  - 巡航ミサイル
  - ドローンで観測しつつ砲兵の間接射撃で更地にする
  - スナイパー派遣?
  - アンテナはさすがに若干離れたところに設置するだろうから、現地の偵察なりでテントの位置特定は必要
- 通信の存在そのものがリスクでしかない
  - 昔の日本陸軍では通信部隊が電話線を架設していたのだが→無線に頼らずに済む



2022年の例3

- 「大きな揚陸艦がロシアが占領した港にやってきて戦車を揚陸しています!!!」
  - TelegramでZvezdaが公式発表(の転載)
    - ロシア側が攻めてるぞ、こんなに武器が来たぞ、というプロパガンダ目的だった模様
  - https://twitter.com/RALee85/status/1505754153146068993

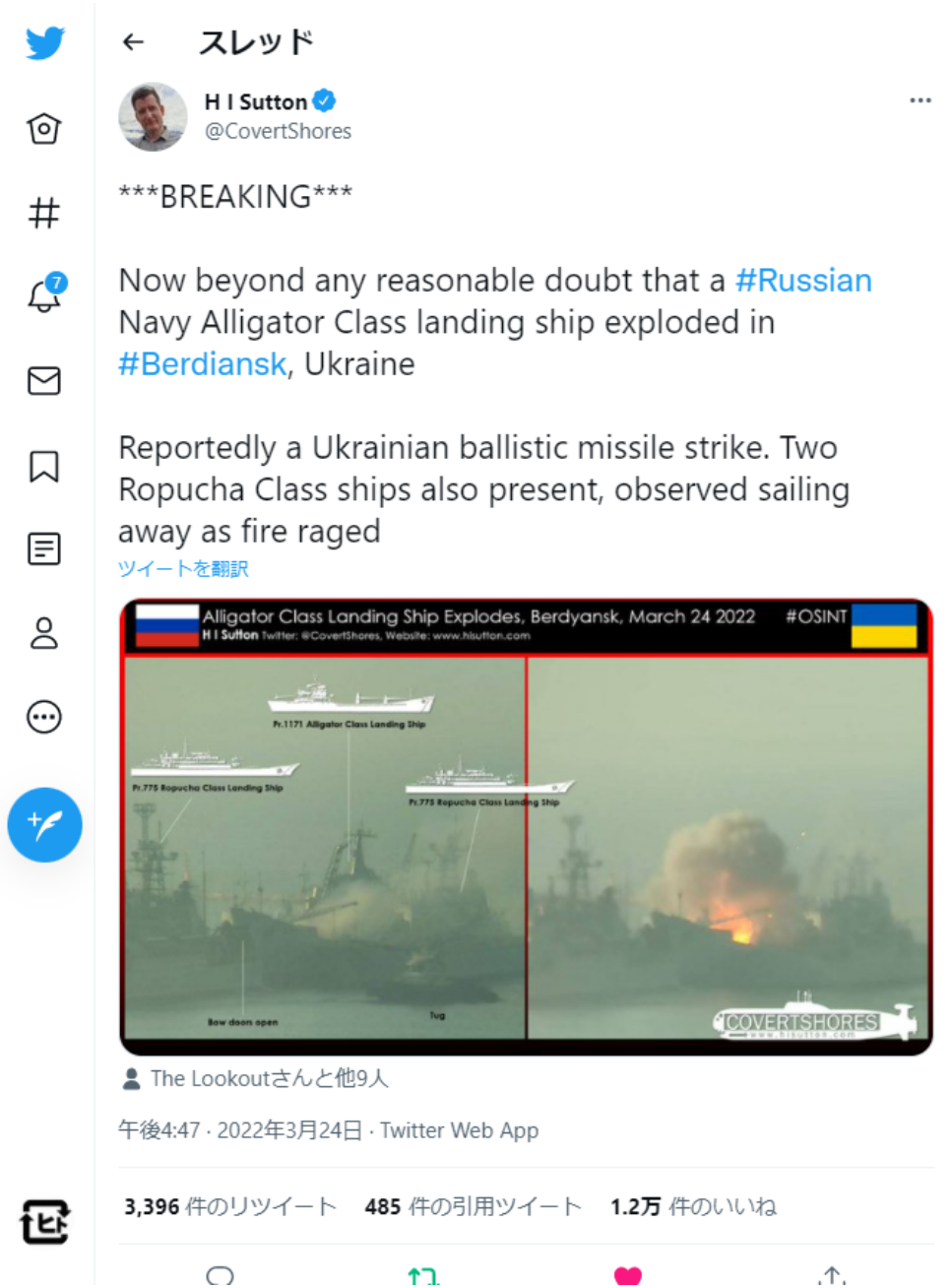


2022年の例3

- 「黒海艦隊の戦車揚陸艦オルスクがベルディヤンスク港でBTR-82A戦闘車を揚陸しています」
  - Telegramに上がった公式の動画(の転載)
  - やっぱり目的はプロパガンダ
  - https://twitter.com/RALee85/status/1505772419906211840

2022年の例3

- 動画からジオロケーション→ウクライナが弾道ミサイル攻撃
  - ベルディヤンスク港のふ頭を特定
  - 通常弾頭・単弾頭中距離ミサイル?
- 戦車揚陸作業中にミサイル着弾
  - 逃げられないので次々誘爆・大火災
  - https://twitter.com/CovertShores/status/1506900560167026690
  - 火気厳禁の作業中に引火→誘爆説もあるが



2022年の例3

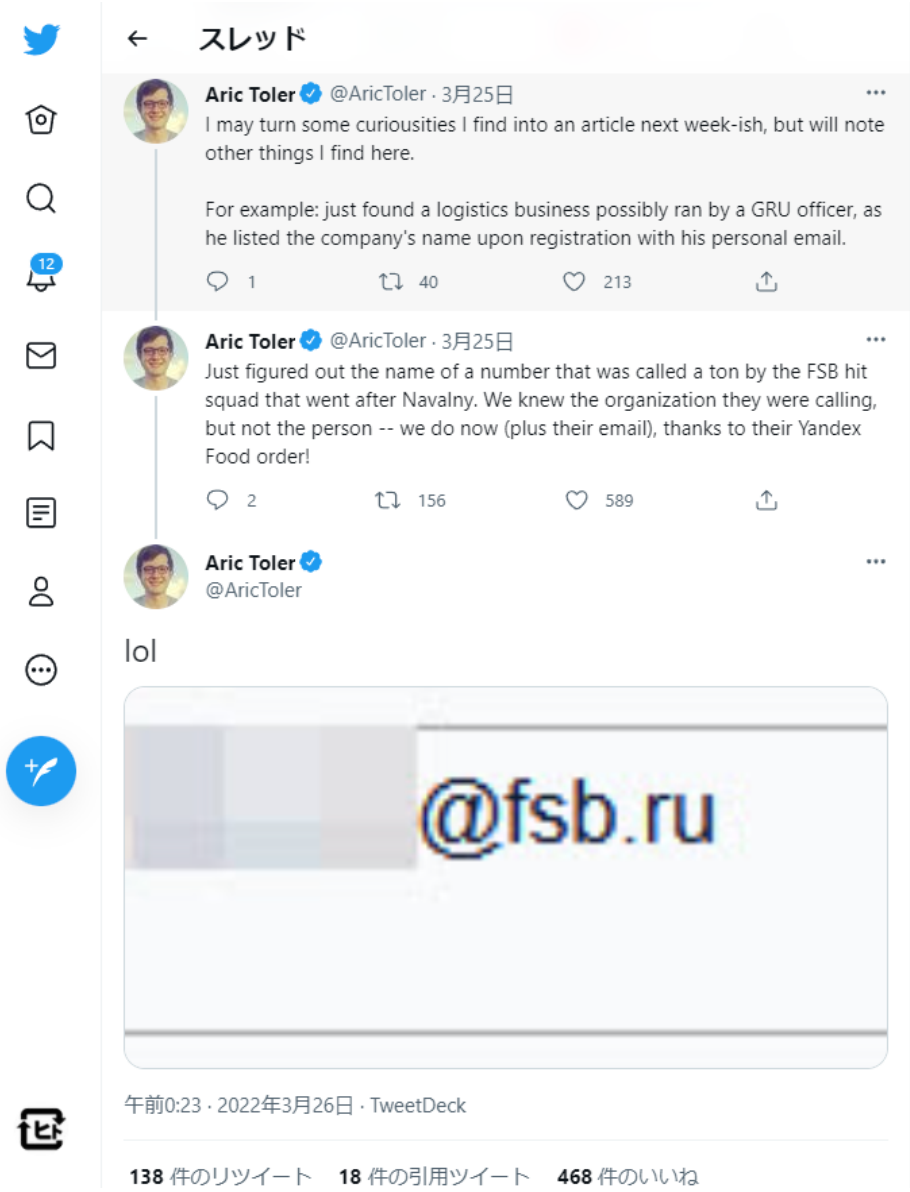
- 最終的に
  - 2隻大火災大破着底
  - 2隻損傷→脱出
  - https://twitter.com/UAWeapons/status/1506963100095889417
    - 揚陸部隊の旗艦に当たったらしいので電波評定かも?
- 接岸している船はすぐに出港できない
  - 311のとき30分で横須賀から全艦緊急出港した海上自衛隊を見て米軍が感心していたそうな

2022年の例3

- 思いっきりバカにされている
  - 動画の情報からジオロケーションに5分～30分
  - ミサイル部隊に連絡5分
  - 座標入力・発射に5分
  - https://twitter.com/tatsurokashi/status/1506930593980096516
- 満載の戦車揚陸艦から荷下ろしするのに必要な時間?
  - LOLO船なのかクレーンがいるのか?
- 荷下ろしをあきらめて緊急出港に要する時間?

2022年の例4

- FSBの職員がフードデリバリーを頼む
- フードデリバリーの会社Yandexにanonymousが攻撃→顧客情報流出
- 顧客情報の中にFSB職員の個人名その他
  - https://twitter.com/AricToler/status/1507031532917207047 で始まるスレッド
  - 非公開だったはずの特殊作戦センターの場所・入り方、etc.が出てきた
- この件は何が教訓なのだろうか???



通信の保安全般について

- ロシアの「やらかし」から何が学べるか?

- これをレポート課題にしようかな～?
  - Enigmaじゃなくてこっちに興味がある人はこっちでもいいことにしよう

ステガノグラフィ

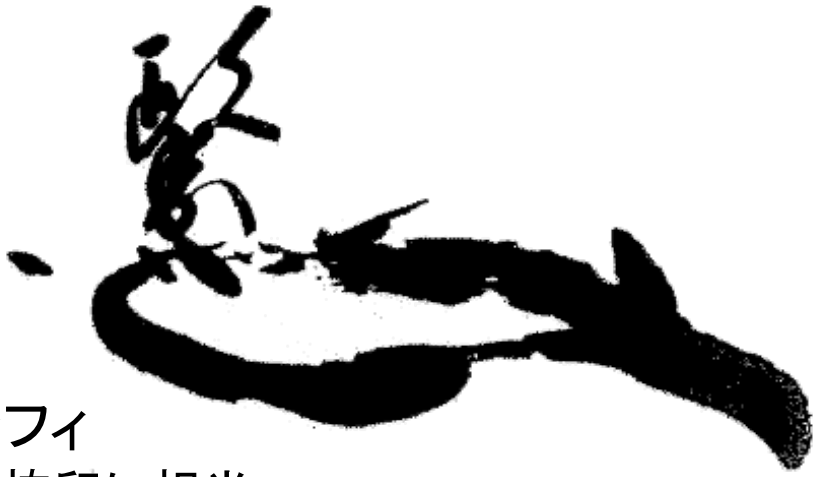
- 「情報の中に情報を隠す」
  - あらかじめ情報を隠す方法・隠した情報を取り出す方法を取り決めておく
    - 情報の受信者がいることは条件ではない。発信者証明として使われたこともある
  - 大抵は送れる情報量は大したことない
  - ステガノグラフィで送る情報自体が暗号化されているかどうかは別問題
    - といっても暗号と併用される場合が多い
- 分類
  - 偽造防止を主眼としたもの; お札のマイクロ文字やUV蛍光インク等
  - 精々数ビット～10ビット程度の情報を送れればよいもの
  - ガチの(大量)通信用

ステガノグラフィ

- 何の変哲もない手紙の行間にあぶり出しインクで別の手紙を書く
  - マリーアントワネットの例
- 紫外線で蛍光を発するが可視光では白色・透明のインクを使用する
  - バリエーション: 可視光では黒・青などのインクにUVで赤蛍光を持つインク
    - 可視光では同じ色調のインクと使い分ける
- 2ch風の大きなアスキーアートに情報を隠す研究
  - 木綿麻実路, 岩切宗利, "冗長化アスキーアート生成法による情報ハイディングとその能力", *情報処理学会論文誌* , No.47, Vol.4, pp. 1258-1265, 2006.
    - 著者は防衛大学校所属
    - 濃淡系のアスキーアートの方が隠しやすい。が、濃淡系自体はあまり使われず目立つ
    - 2KBの濃淡系AAに対して438B埋め込め、AAの品質を損なわないことが報告されている
- 言い回しや同義語を使用して情報を文書に隠す研究
  - 中川 裕志, 滝澤 修, 井上 信吾, “ドキュメントへのインフォメーションハイディング”, 特集インフォメーションハイディング, *情報処理*, Vol.44, No.3, pp.248-253, 2003.

ステガノグラフィ

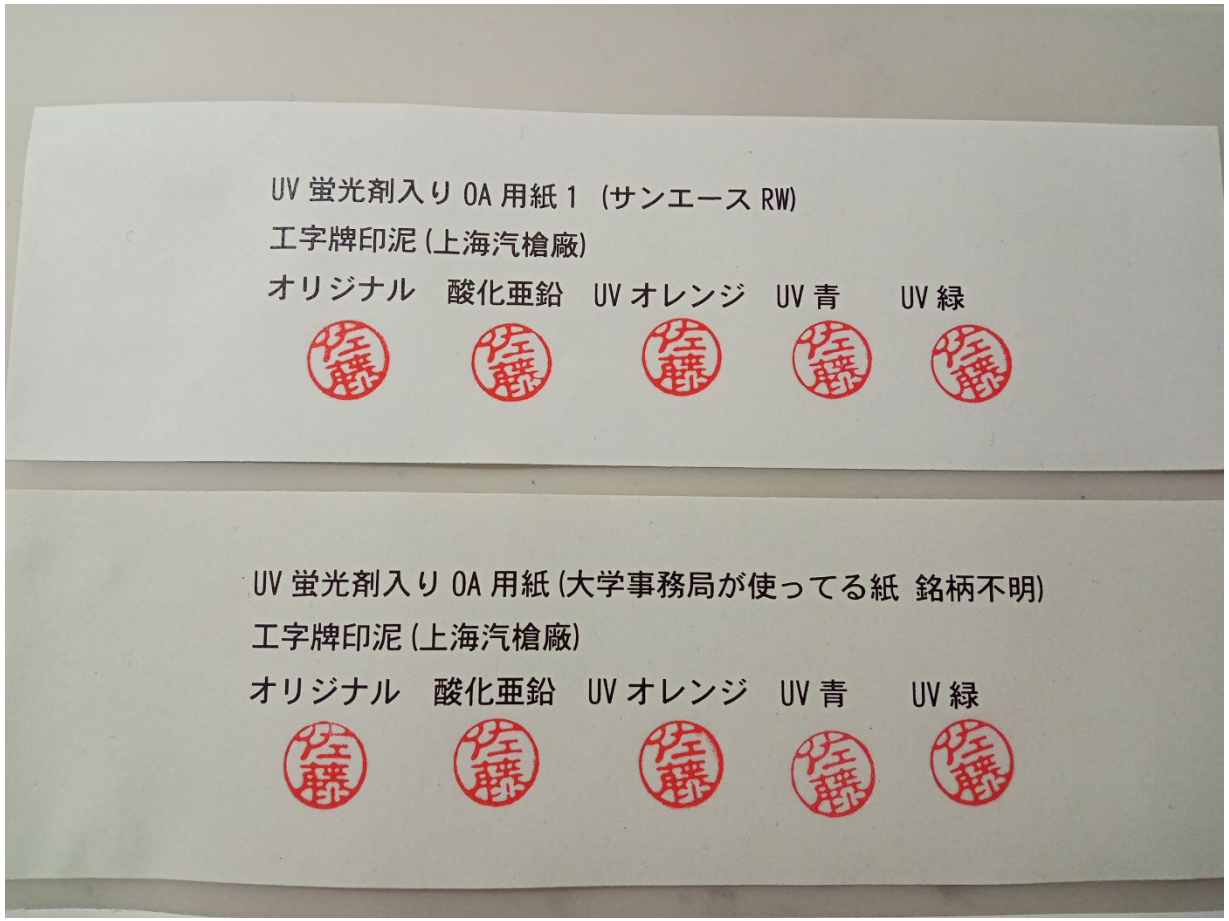
- 画像・動画等への著作権情報・シリアルナンバー埋め込み
  - ストリーミング・ダウンロード販売の違法コピー対策
  - JPEG・MP3のような不可逆圧縮に知覚できないように情報を埋め込む方法がいくつか実用になっている
    - コメント用領域とは別。購入・ユーザごとに一方向ハッシュ値が違うのでわかる
    - グラデーションの微妙な違いは認識困難etc
    - 大きな音の周波数の近傍に小さな音は認識困難etc
- 伊達政宗の花押(諸説あってかなり怪しい)
  - 政宗を崩しつつ鳥の絵が書いてある
  - 政宗自身はセキレイといっている
  - セキレイの目に針で穴をあけた(本当か怪しい)
  - 真の署名を示す1ビットの情報だと思えばステガノグラフィ
    - 花押: 江戸期のどこかまでは武士の間では今でいう自署+捺印に相当
    - 農民は印鑑だったらしい



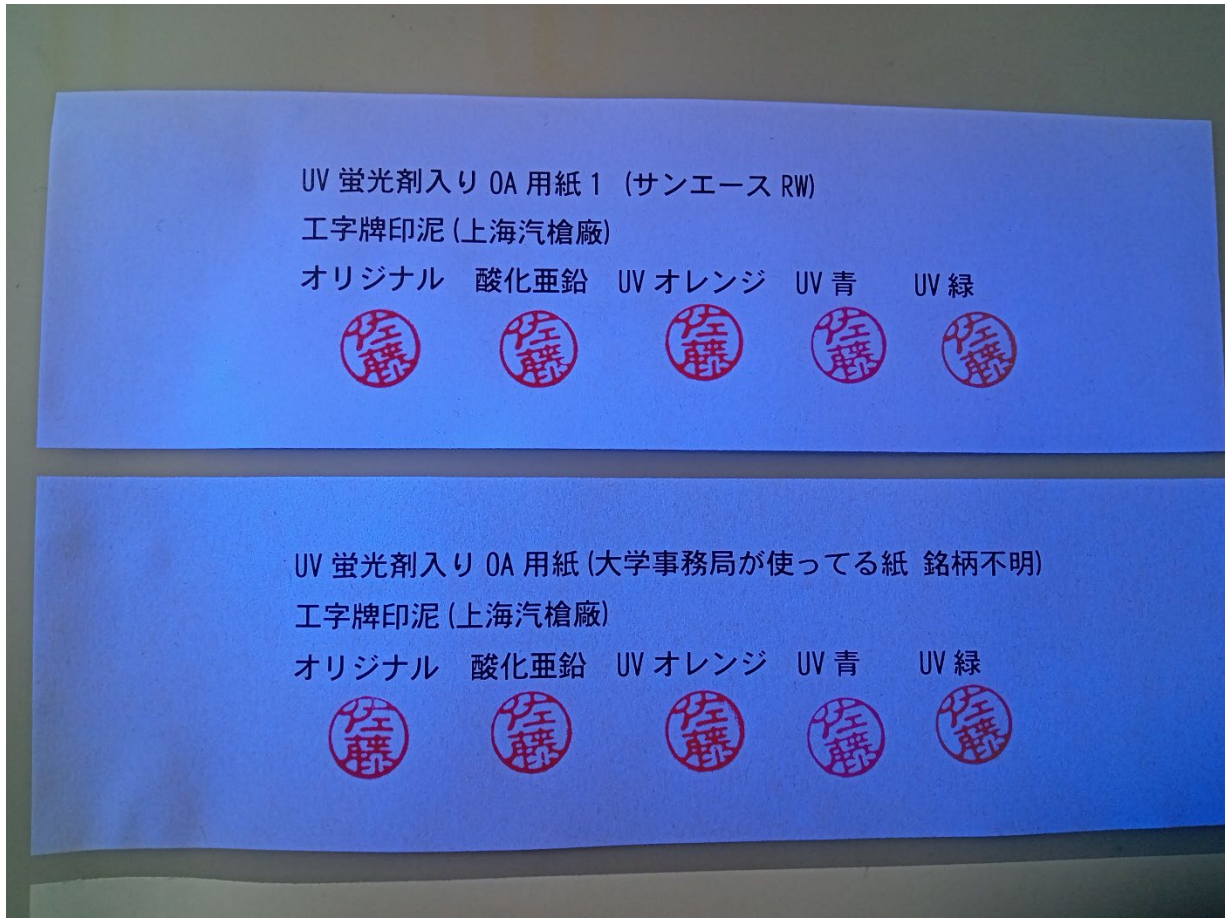
ステガノグラフィ

- あぶり出しとか消えるインクとかであそんでみよう
  - ガラスペン、レモン汁、電熱器orろうそくを用意
- 消えるインク: 塩化コバルト(II)六水和物水溶液(長田順行, 暗号大全)
  - 水で塗れるとピンク～赤、乾燥すると青; 主に第1次大戦期に使われた
    - コップ1杯の水に1/2さじを溶かす→薄ピンクの液ができる
    - 加熱して乾燥させると水色に発色、放置すると空気中の水分を吸収してピンクに戻る
    - なお、UVでうっすら見える模様
- UVインクが開発されたのは戦後
  - UV顔料を混ぜた印泥を作ったぞ
  - UV顔料を混ぜた万年筆用インクも作ったぞ
  - 無機UV顔料は耐熱性があるが比重が3以上ある→すぐ沈殿してしまう
    - ペンキに混ぜる・陶器の釉薬向けなので万年筆にはちょっと向いていないかも?

ステガノグラフィ(というより偽造防止?)

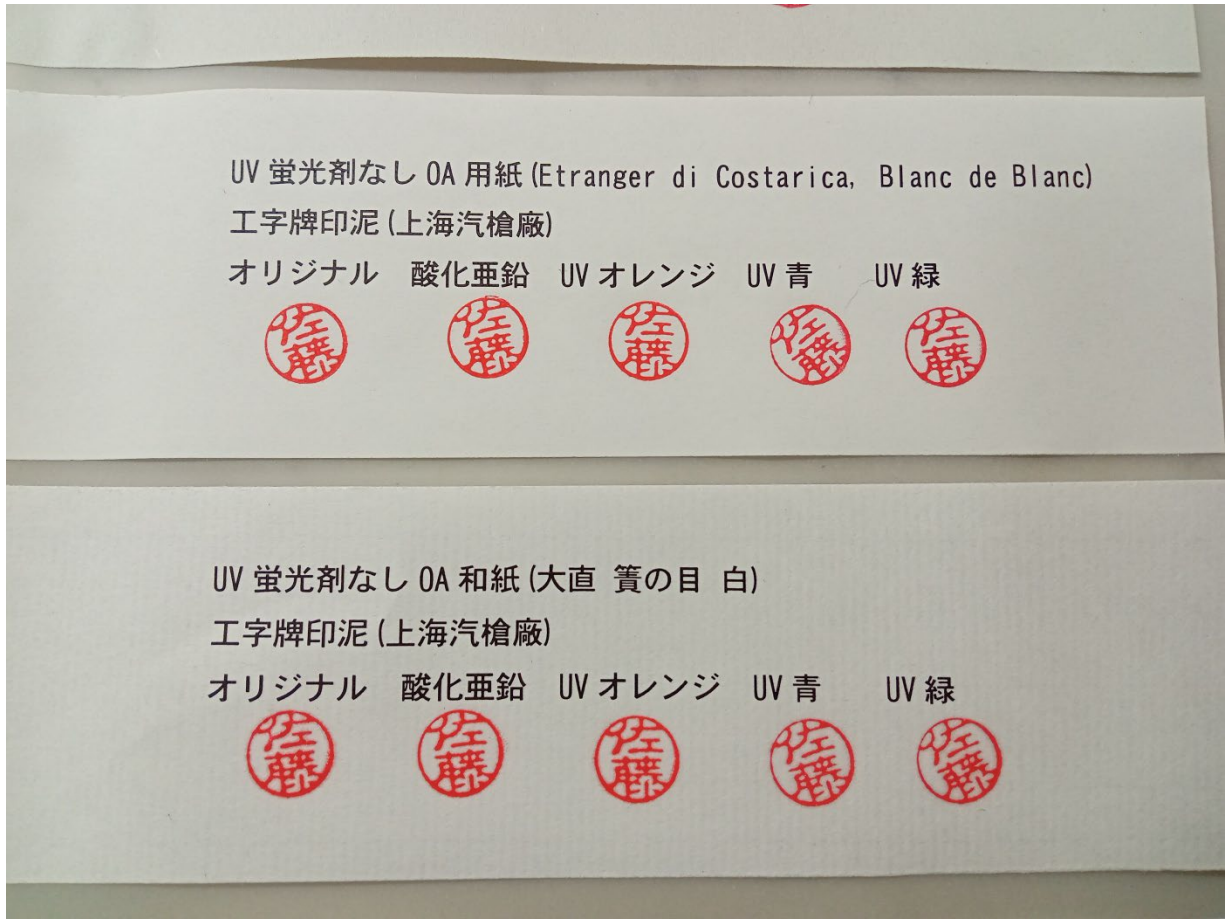


可視光(昼白色蛍光灯)

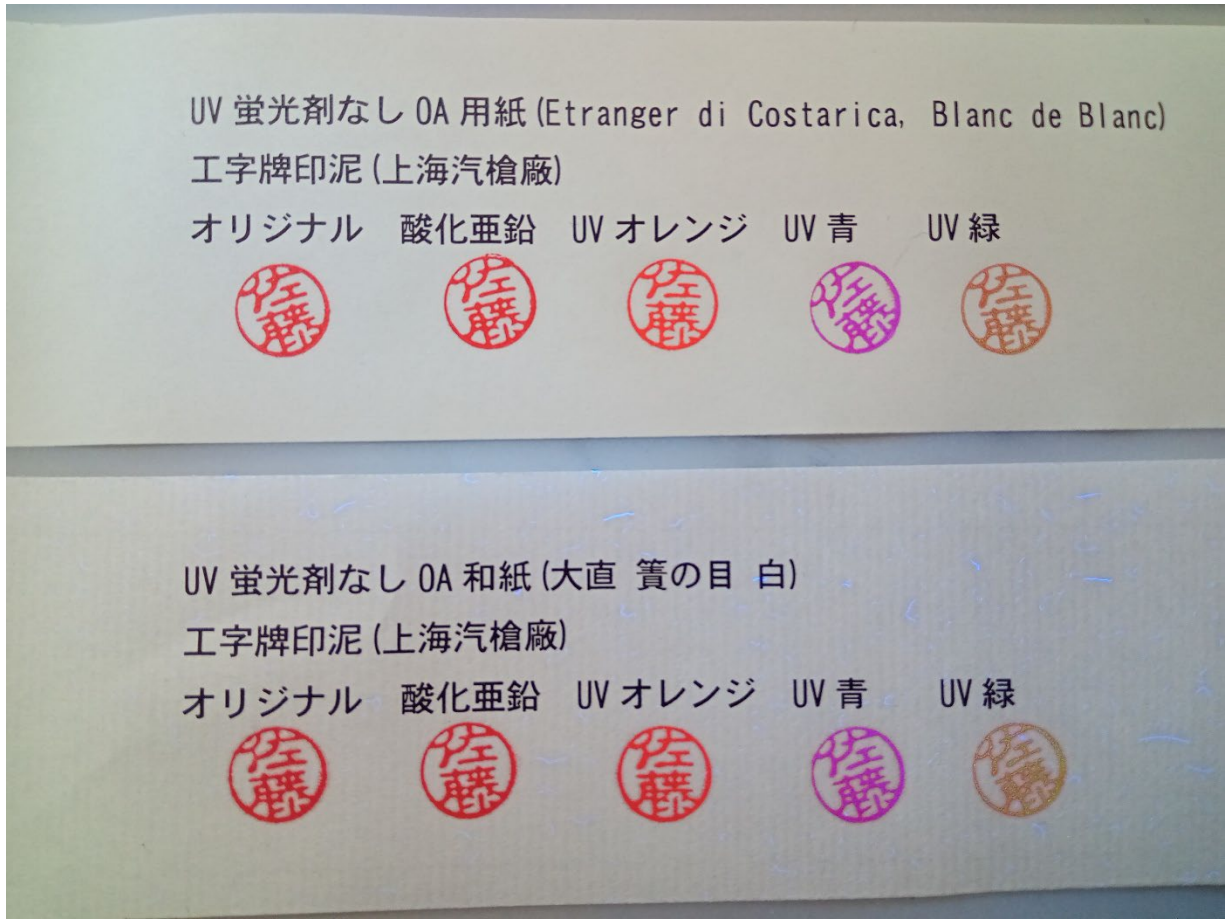


紫外線 365nm

ステガノグラフィ(というより偽造防止?)

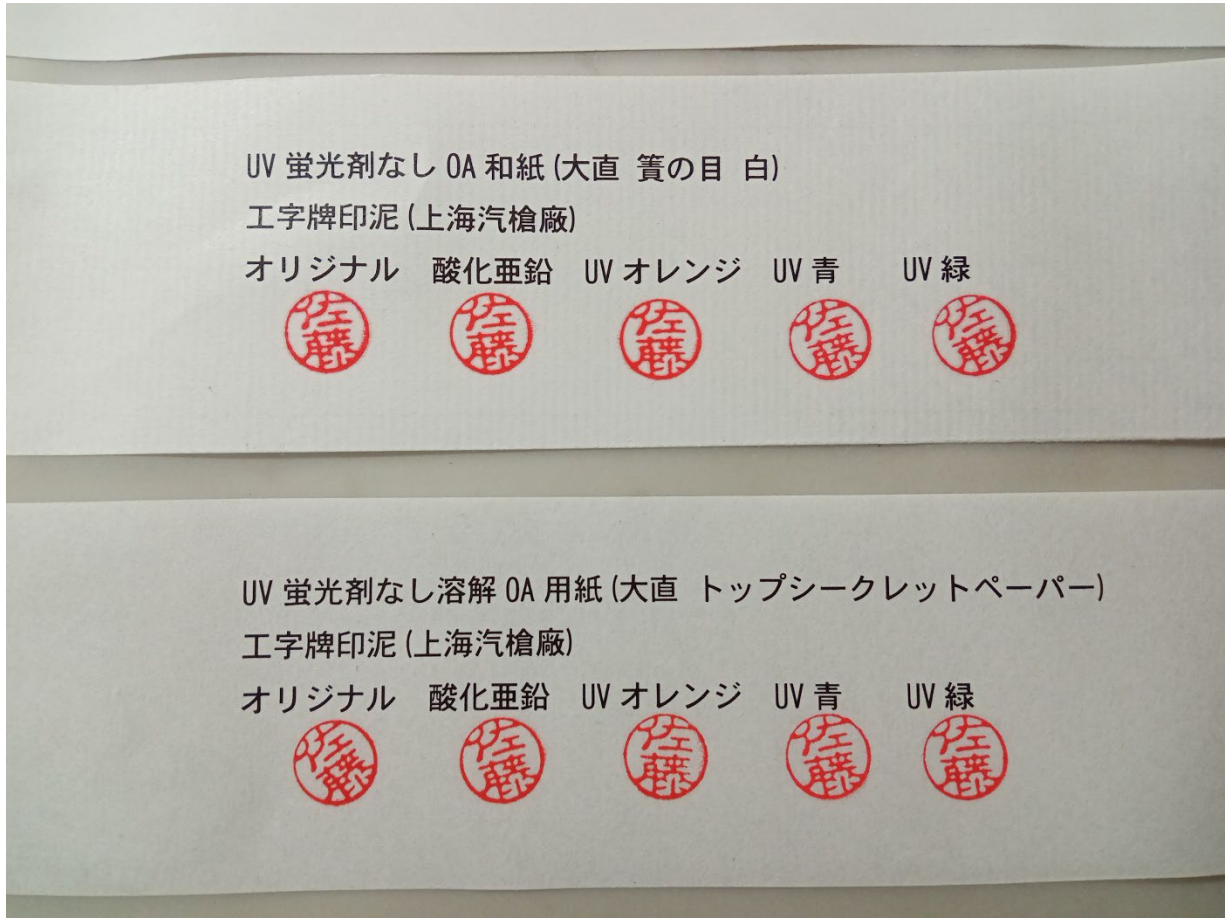


可視光(昼白色蛍光灯)

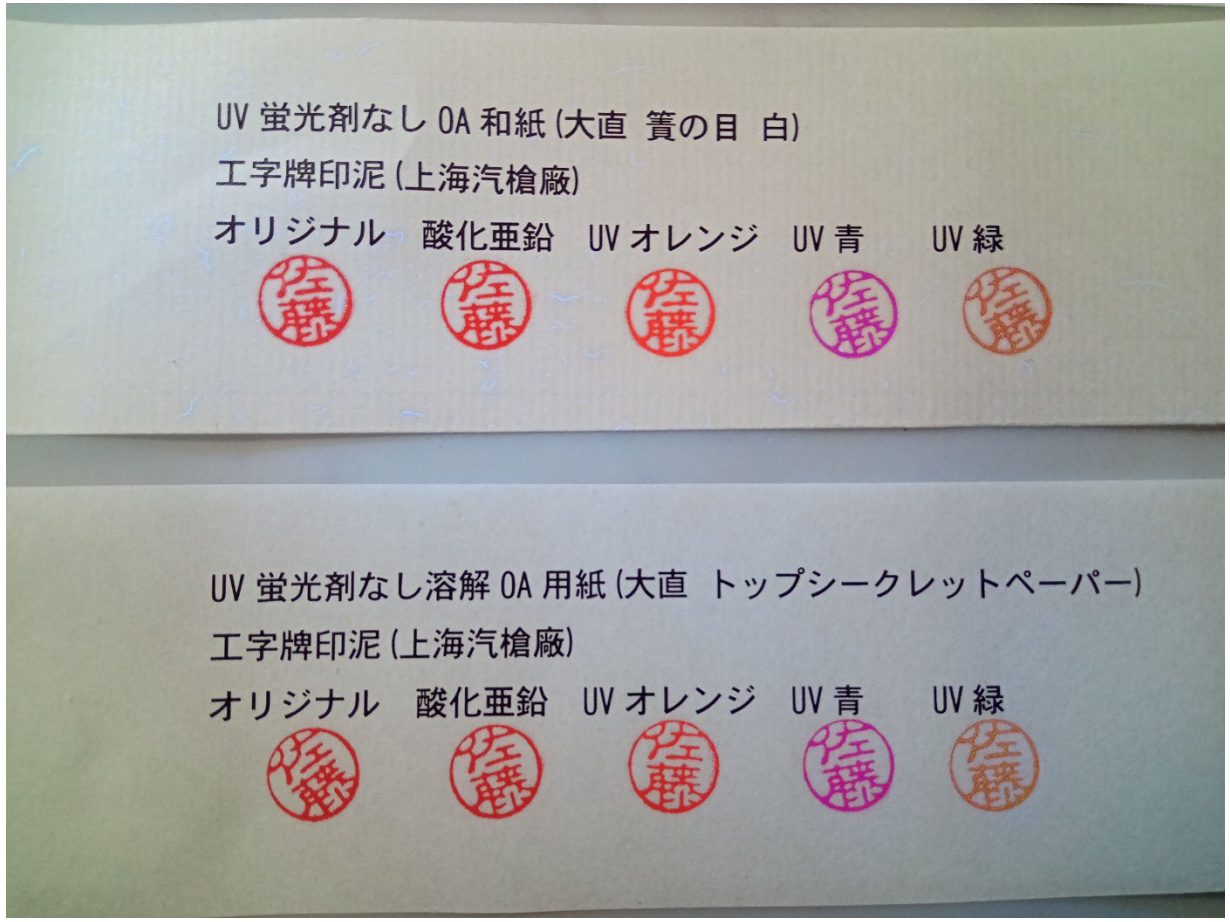


紫外線 365nm

ステガノグラフィ(というより偽造防止?)



可視光(昼白色蛍光灯)



紫外線 365nm

にんげんだもの…。

- 情報システムといっても、ハードウェア・ソフトウェアだけではない
  - ハードウェアにはここではサーバ・機器類を収容する建築物やら何やらをすべて含む
- 人間が一番弱い
  - 作るのも人間、運用するのも人間、改善・変更するのも人間
  - 人間を信用してはいけない
    - 面倒がる、悪意を持って組織内にもぐりこんだ人、そもそも理解できてない人、色々いる
- 管理・運用している情報システムが安全だと考えるのも危険
  - システムそのものが現に安全だとする
  - が、そのうち安全が神話になる→システムそのものが安全でなくなったときに安全と信じられ続けてしまう

にんげんだもの…。

- 人間を信用してはいけない
  - 自分も信用してはいけない