警察庁技官の仕事

警察庁サイバー警察局情報技術解析課

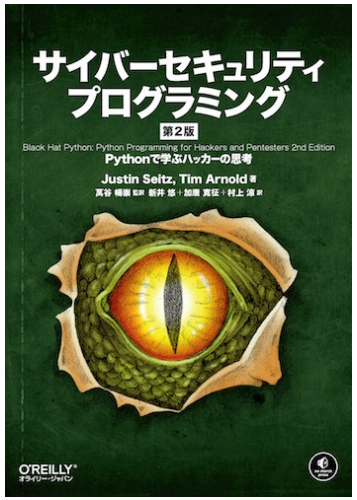
萬谷 暢崇

自己紹介

- 萬谷 暢崇(まんたに のぶたか)
- 警察庁技官(国家公務員一般職)
- 警察庁サイバー警察局情報技術解析課
  サイバーテロ対策技術室(サイバーフォースセンター)専門官
- 警察庁指定広域技能指導官(情報技術の解析)
- 担当業務
  - ソフトウェアの脆弱性や新しいサイバー攻撃手法と
    その対策に関する情報収集、分析

自己紹介

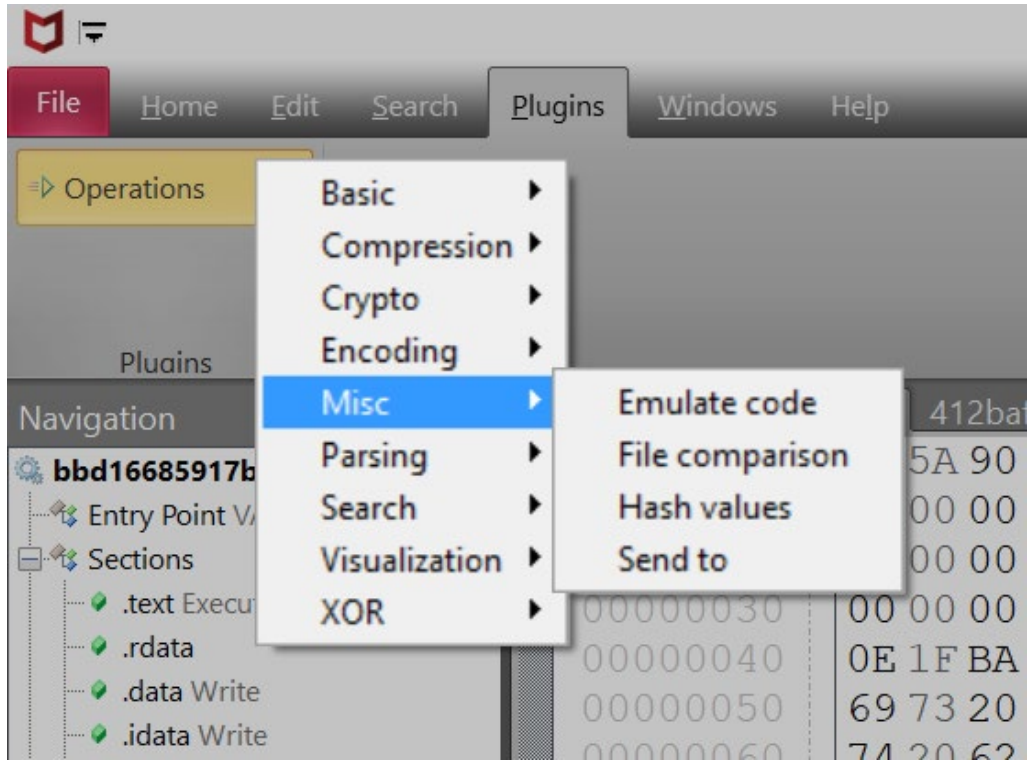
- プライベートでの活動
  - FreeBSD Project メンバー
    （ports committer, 2001～）
  - サイバーセキュリティプログラミング 第2版
    （オライリー・ジャパン, 2022） 監訳
  - マスタリングLinuxシェルスクリプト 第2版
    （オライリー・ジャパン, 2022） 監訳

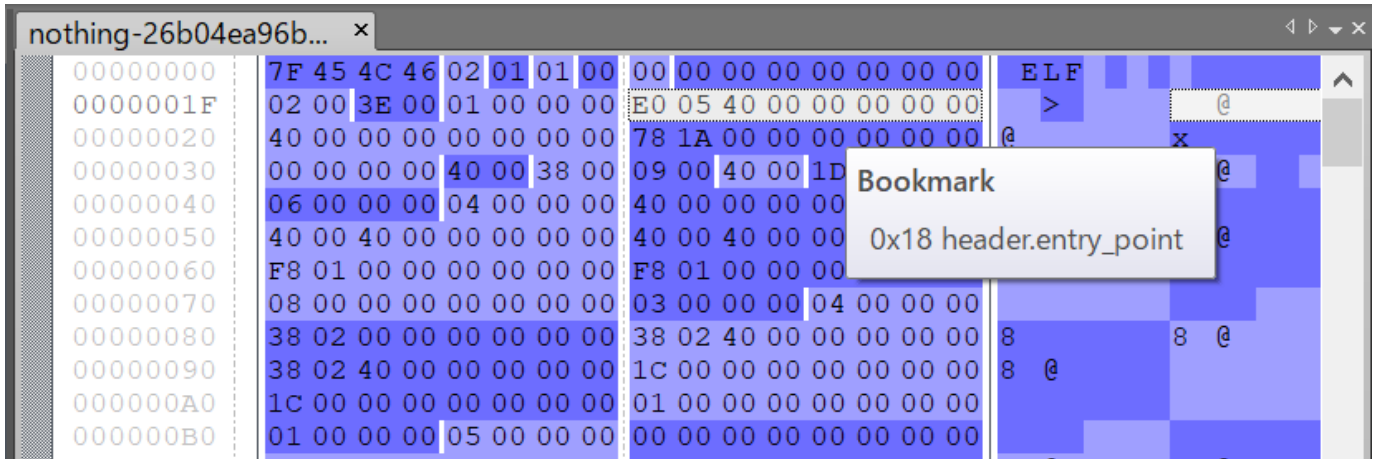


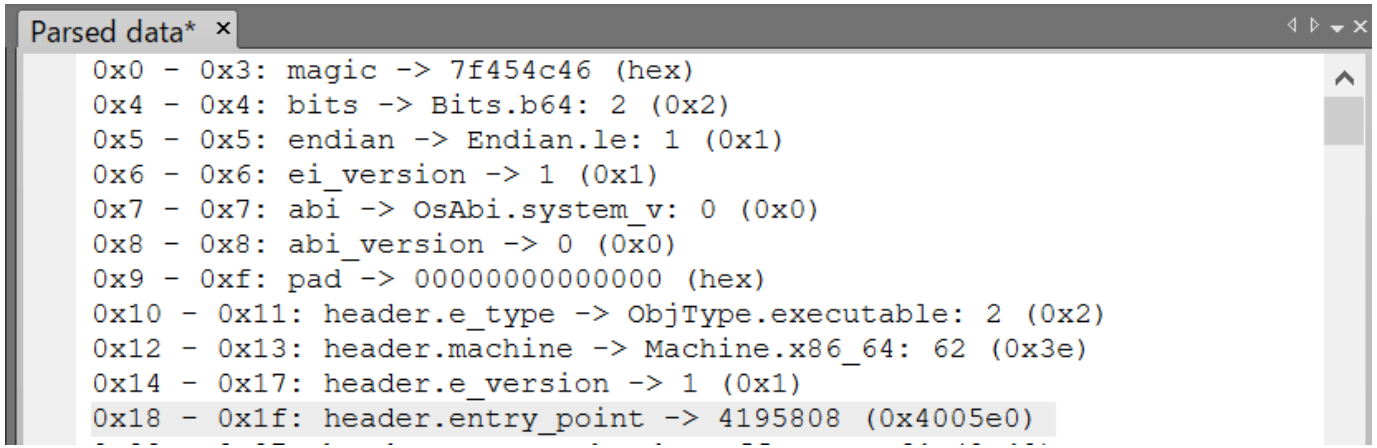
自己紹介

- プライベートでの活動
  - オープンソースソフトウェアの開発
    - FileInsight-plugins
      - McAfee FileInsightバイナリエディタのマルウェア解析用Pythonプラグイン集（約130個）
      - 18種類の圧縮アルゴリズム、10種類の暗号アルゴリズム、20種類のエンコード方式に対応
        https://github.com/nmantani/FileInsight-plugins/README.ja.md

自己紹介


File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Emulate code
File comparison
Hash values
Send to
Navigation
bbd16685917b
Entry Point V
Sections
.text Execu
.rdata
.data Write
.idata Write


nothing-26b04ea96b...
00000000 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00 ELF
0000001F 02 00 3E 00 01 00 00 00 E0 05 40 00 00 00 00 00 >
00000020 40 00 00 00 00 00 00 00 78 1A 00 00 00 00 00 00 @ x
00000030 00 00 00 00 40 00 38 00 09 00 40 00 1D
00000040 06 00 00 00 04 00 00 00 40 00 00 00 00
00000050 40 00 40 00 00 00 00 00 40 00 40 00 00
00000060 F8 01 00 00 00 00 00 00 F8 01 00 00 00
00000070 08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00
00000080 38 02 00 00 00 00 00 00 38 02 40 00 00 00 00 00 8 8 @
00000090 38 02 40 00 00 00 00 00 1C 00 00 00 00 00 00 00 8 @
000000A0 1C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
000000B0 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00
Bookmark
0x18 header.entry_point


Parsed data*
0x0 - 0x3: magic -> 7f454c46 (hex)
0x4 - 0x4: bits -> Bits.b64: 2 (0x2)
0x5 - 0x5: endian -> Endian.le: 1 (0x1)
0x6 - 0x6: ei_version -> 1 (0x1)
0x7 - 0x7: abi -> OsAbi.system_v: 0 (0x0)
0x8 - 0x8: abi_version -> 0 (0x0)
0x9 - 0xf: pad -> 00000000000000 (hex)
0x10 - 0x11: header.e_type -> ObjType.executable: 2 (0x2)
0x12 - 0x13: header.machine -> Machine.x86_64: 62 (0x3e)
0x14 - 0x17: header.e_version -> 1 (0x1)
0x18 - 0x1f: header.entry_point -> 4195808 (0x4005e0)

業務内容

- ソフトウェアの脆弱性や新しいサイバー攻撃手法についてインターネット上の情報を収集
- 影響範囲、攻撃発生の有無、対策等の情報をまとめた技術資料を作成
- 動作検証可能なものについては動作検証を行って攻撃時に残る痕跡や対策の有効性を確認

業務の事例

- Spring Frameworkのリモートコード実行の脆弱性（CVE-2022-22965：通称 Spring4Shell）
- Spring Framework
  - Javaベースのオープンソースのアプリケーションフレームワーク
- Spring4Shellの脆弱性
  - Spring Frameworkを使用しているウェブアプリケーションに細工したHTTPリクエストを与えることで任意のコードを実行可能
  - **ウェブサーバへの侵入、マルウェア感染等の被害のおそれ**

業務の事例

Spring Frameworkの開発元のVMware社が脆弱性の情報を公開

Twitterやセキュリティベンダーのブログ等で関連情報を収集、深刻度や影響範囲を確認

攻撃の検証コード（Proof of Concept：PoC）がGitHub で公開されていることを確認

収集、分析した情報をまとめた資料を作成、展開しつつ PoC の検証環境を構築して動作検証を実施

過去の仕事

警察庁の地方機関

- 警察本部の国費整備の内線電話や情報通信システムの維持管理
- 捜査で押収された携帯電話やPCの解析(デジタルフォレンジック)

他省庁

- 内閣サイバーセキュリティセンター(NISC)でマルウェア解析

警察大学校

- サイバー犯罪捜査に従事する警察官向け研修コースの教官
- 実習環境の構築、技術的なトピックについての講義

警察に入って今の仕事をするまで

- コンピュータは大学生になってから触り始めた
- 学生の頃からプログラムを書くのが好き
  - PerlやPHPでウェブアプリを作成
  - FreeBSD 用の各種ソフトウェアのパッケージ（ports）をメンテナンス、1998年からパッチを送り続けて2001年から ports committerに
- 警察に入ったきっかけ
  - たまたまウェブサイトで業務内容の紹介を見て
- セキュリティの仕事をするようになったきっかけ
  - 採用3年目に警察庁のサイバーテロ対策技術室に異動してから

警察庁技官の様々な仕事（情報技術解析）

都道府県警察の捜査で押収された電子機器の解析等の捜査支援

サイバー攻撃の被害を受けたコンピュータやマルウェアの解析

警察庁一般職技術系採用パンフレット
https://www.npa.go.jp/joutuu/saiyou2/2syugijyutukeisaiyou/2022_ippansyoku-gijyutu_punfu.pdf

警察庁技官の様々な仕事（機動通信）

事件、事故、災害等の現場での通信確保と映像伝送

無線中継所等の通信施設や
警察情報通信システムの維持管理

警察庁一般職技術系採用パンフレット
https://www.npa.go.jp/joutuu/saiyou2/2syugijyutukeisaiyou/2022_ippansyoku-gijyutu_punfu.pdf

警察庁技官の様々な仕事（通信施設）

無線中継所等の通信施設の整備

全国を結ぶ警察基幹通信網の整備

警察庁一般職技術系採用パンフレット
https://www.npa.go.jp/joutuu/saiyou2/2syugijyutukeisaiyou/2022_ippansyoku-gijyutu_punfu.pdf

警察庁技官の環境

概ね3～5年周期で異動

採用された管区（地方）を中心に転勤

都道府県警察、他省庁への出向も

技術的な業務
＋
事務的な業務

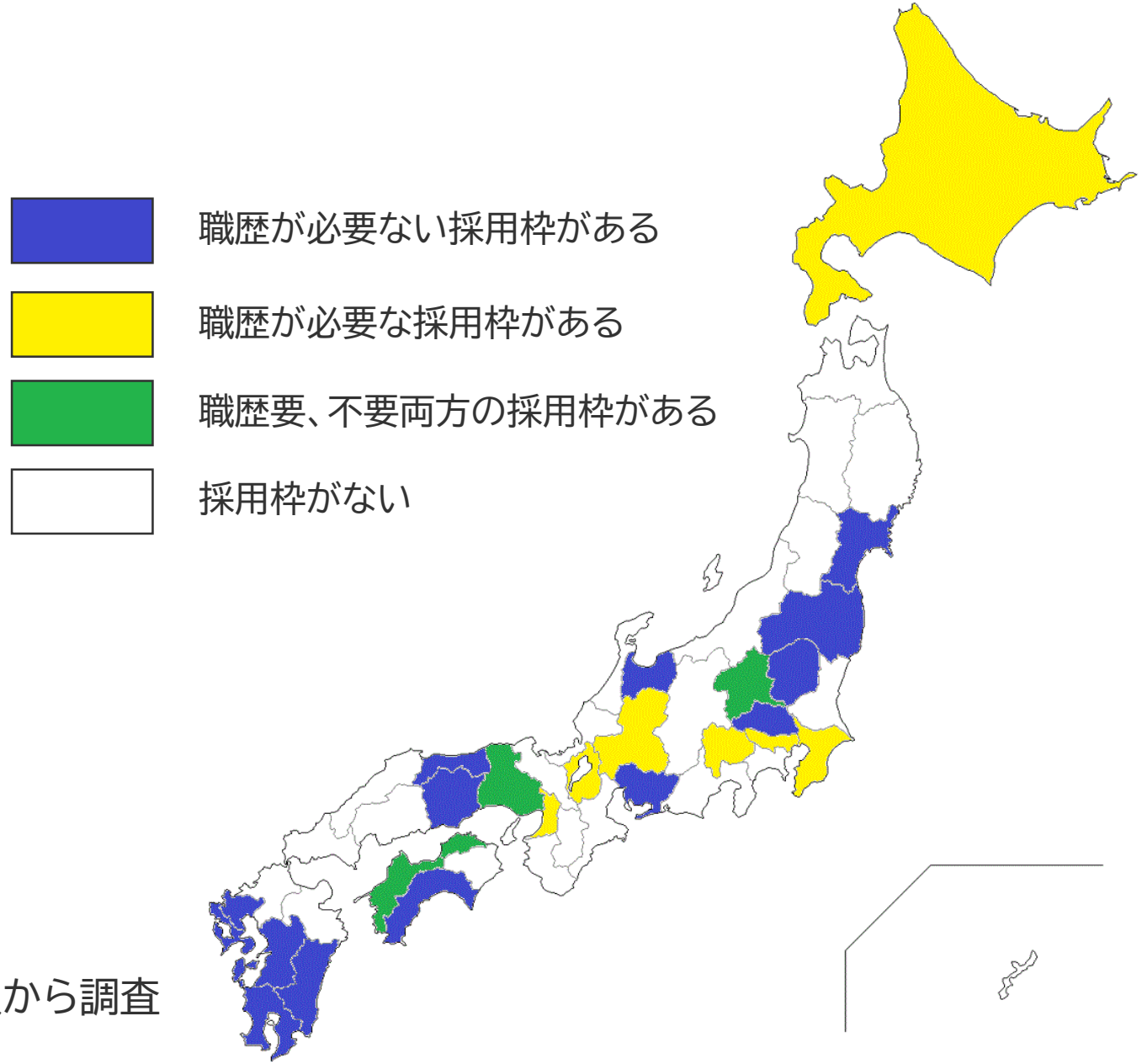
技術によって国民の安全・安心に貢献

サイバー捜査官

- 都道府県警察の警察官（地方公務員）
- 採用された都道府県で勤務
  （警察庁等へ出向する場合もあり）
- サイバー特別捜査官等の採用枠
  - 主にサイバー犯罪捜査に従事、昇任等のタイミングで一時的に別の業務に従事することも
- 一般の警察官の採用枠
  - サイバー犯罪捜査に従事できるとは限らない

サイバー捜査官

- 採用枠は1～2名が多い
- 受験資格に情報処理安全確保支援士や情報処理技術者の資格を必要とするところが多い
- 試験に身体検査（視力、色覚等）や体力検査がある



※ 都道府県警察ウェブサイトの令和4年度採用情報から調査

白地図データ：CraftMAP（http://www.craftmap.box-i.net/）

警察庁採用情報（一般職技術系情報通信職員）
https://www.npa.go.jp/joutuu/saiyou2/2syugijyutukeisaiyou.htm

都道府県警察官採用案内
https://www.npa.go.jp/about/recruitment/police/index.htm