ITは農業を援け、セキュリティはそれを守れるのか

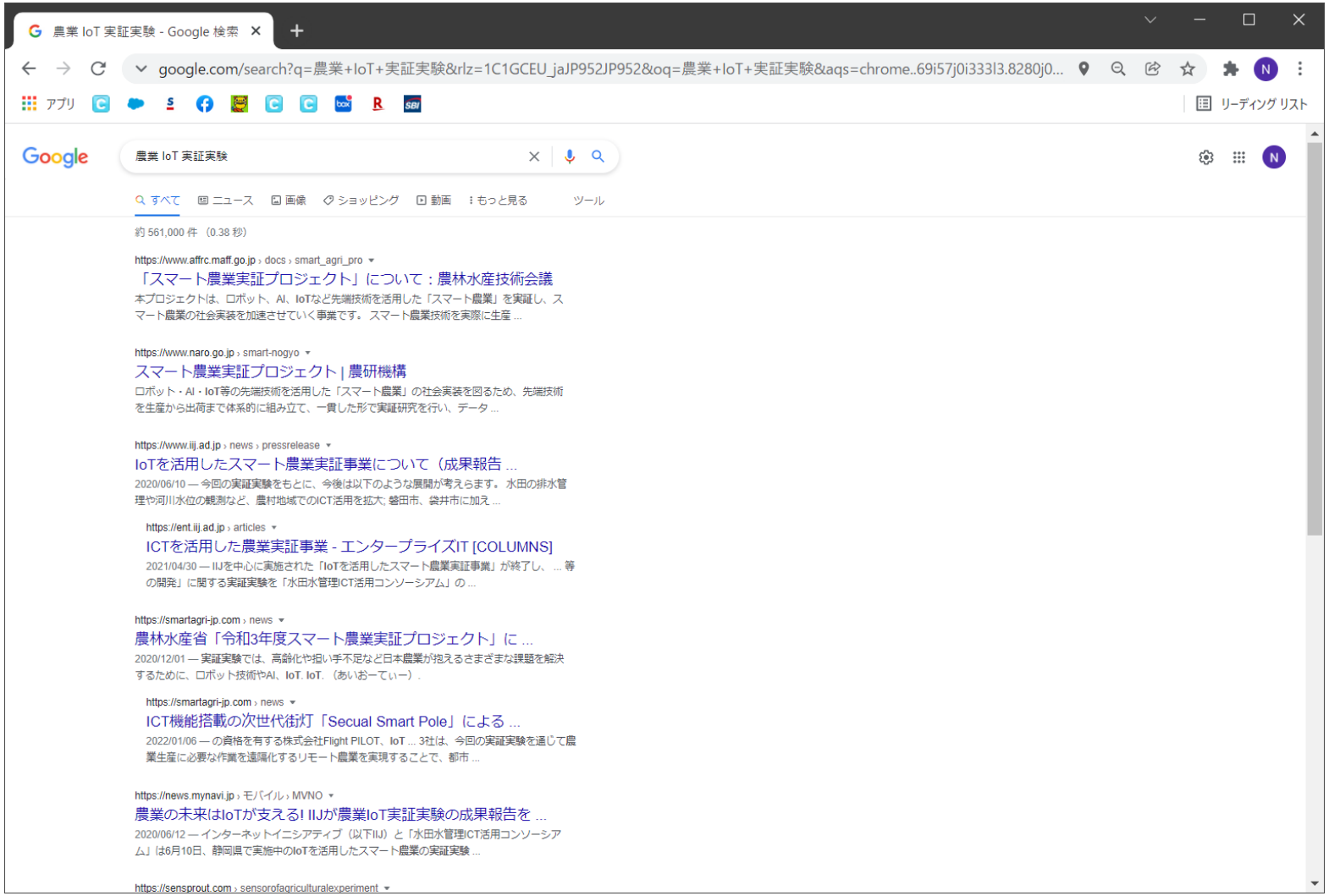
株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp/

2022年1月28日 @online

農業の課題

- 人手不足
- 権利者問題
- IT化・ IoT化で効率アップ（？）
- 経済的な問題（採算が取れるのか？）

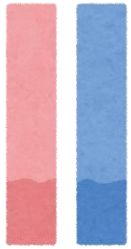
農業IoT化、調べてみた



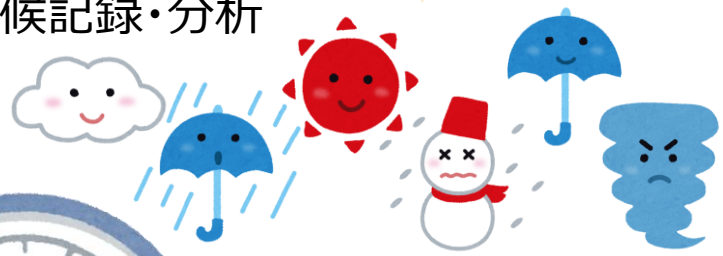
農業IoT化

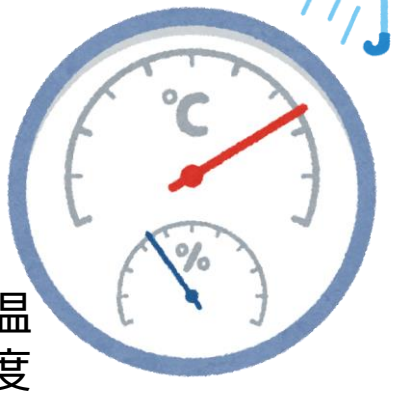
水管理

pH



天候記録・分析

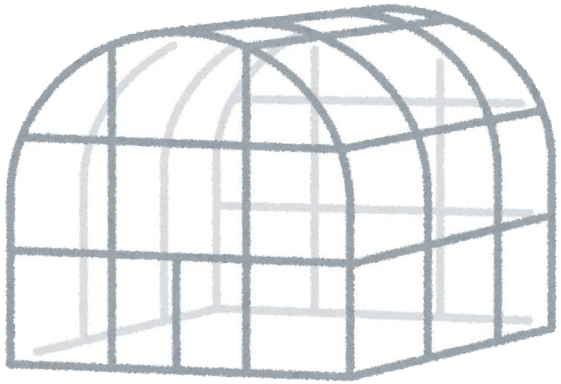




気温、室温
温度、湿度

防犯、盗難対策
無人運行

ドローン活用



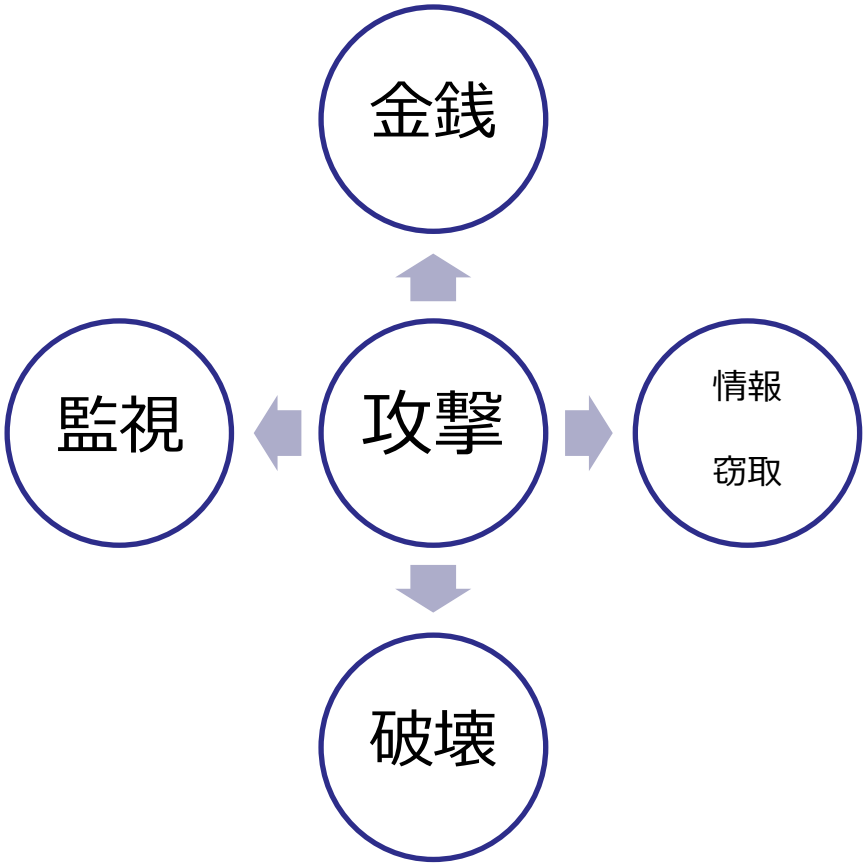
データはどこに。

- センサー類、IoT機器から取得できるデータやログ
  - 蓄積 → 分析 → 現場に還元・実践、この繰り返し
  - 蓄積データとその活用は、ノウハウそのもの

- Open v.s. Close
  - 情報を開示する メリット・デメリット
  - 情報を秘密にする メリット・デメリット

- データの重要性（重要性≒機密性）
  - あなた、あるいは御社にとって重要なデータ
  - 攻撃者が欲しいデータ

サイバー攻撃の意図と目的



個人情報

- 個人情報を保持しているか否か
  - 個人・家族経営
  - 事業体・法人
- 個人情報の保管場所
- セキュリティポリシー
  - そもそも策定しているか（策定できるか）
  - 策定している場合でも、実効性のある運用ができているか
  - 監査は適切か
- 2022年4月施行 改正個人情報保護法

改正個人情報保護法(2022年4月施行)のポイント

1. 本人の請求権の拡大
   - 不適正な利用がなされたときも利用停止等が請求できる、等
2. 事業者の責務の追加
   - 個人データの漏えい等が発生した場合の報告義務及び本人に対する通知義務が新設
   - 個人情報取扱事業者の個人情報の不適正な利用の禁止義務が明文化
3. 事業者の自主的な取り組みの推進
   - 企業の特定分野を対象とする団体の認定団体制度が新設)
4. データ利活用の促進
   - 仮名加工情報(他の情報と照合しない限り個人を特定できないように個人情報を加工した情報)は、内部分析目的の利用に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和
   - 提供元では個人データではないものの、提供先で個人データとなることが想定される場合、提供先に、本人の同意が得られているか等の確認義務を負う(例：cookieの取り扱い等)
5. 罰則強化
   - 措置命令違反：「6か月以下の懲役又は30万円以下の罰金」→「1年以下の懲役又は100万円以下の罰金」
   - 報告義務違反：「30万円以下の罰金」から「50万円以下の罰金」
   - 法人に対する罰金刑を引き上げ：措置命令違反と個人情報データベース等の不正流用については「1億円以下」に
- 域外適用等の拡充
  - 外国の事業者に対する、報告徴収・立入検査などの罰則が追加

株式会社ＦＦＲＩセキュリティ

会 社 紹 介

FFRI Security, Inc.

https://www.ffri.jp

Ver2.00.47

会社概要

会社名：	株式会社ＦＦＲＩセキュリティ（東証マザーズ：3692）
代表者：	代表取締役社長　鵜飼　裕司
所在地：	東京都千代田区丸の内３丁目３番１号　新東京ビル２階
設立：	2007年7月3日
資本金：	2億8,613万6,500円（2019年3月31日現在）
事業内容：	1. コンピュータセキュリティの研究、コンサルティング、情報提供、教育 2. ネットワークシステムの研究、コンサルティング、情報提供、教育 3. コンピュータソフトウェア及びコンピュータプログラムの企画、開発、販売、リース、保守、管理、運営及びこれらに関する著作権、出版権、特許権、実用新案権、商標権、意匠権等の財産権取得、譲渡、貸与及び管理 4. 上記事業に関連する一切の業務

事業概要

サイバー セキュリティ領域でのシーズ型R&D

- 標的型攻撃などに利用されるセキュリティ脆弱性研究、対策技術開発
  100を超える日本最多のクリティカルなセキュリティ脆弱性発見の実績
- 標的型攻撃マルウェアに関する研究、対策技術開発
  標的型攻撃など近年のマルウェア対策に関する研究成果を多数発表
- 組み込みセキュリティ
  組込みシステムのセキュリティ脆弱性脅威分析に関する研究成果を多数発表

製品開発

- 標的型攻撃対策ソフトウェア
- マルウェア自動解析ツール
- MITB攻撃対策ソフトウェア
- 組み込み機器セキュリティ検査ツール
- P2Pシステムセキュリティ製品
- Android用セキュリティ診断アプリ

サービス

- 標的型攻撃マルウェア調査分析
- IoTデバイスのセキュリティ検査
- セキュリティ対策コンサルティング
- 受託研究開発
- Black URL提供サービス
- セキュリティ技術者向けトレーニング

セキュリティ脆弱性研究、対策技術開発

100を超える日本最多のクリティカルなセキュリティ脆弱性発見の実績

セキュリティ脆弱性対策研究に関する実績

- BlackHat USA/Japan、RSA Conference、CODE BLUEなど多数の国際カンファレンスで脆弱性分析に関する研究を発表。
- https://www.ffri.jp/research/index.htm にて多数の研究成果を発表。

セキュリティ脆弱性発見に関する実績

100を超えるクリティカル脆弱性発見の実績有り

例: Microsoft Windows (LSASS脆弱性、wkssvc脆弱性、アニメーションカーソル脆弱性、GDI脆弱性、Office製品、Internet Explorer など多数)、Winny、一太郎、QuickTime、Realplayerなど他多数

記事、専門雑誌、新聞、NHKニュースなどメディアに多数掲載。

例：Windows標準搭載のIPv6スタックに脆弱性発見

報告日:2010年3月24日/公開日:2010年8月11日

その他

・世界で初めてサードパーティ・ベンダーとしてWindows 10のセキュリティリスクに関する検証結果を公開
・世界で初めてWindows 9xシステム安定攻略の可能性を証明
・国内においても多数の研究発表実績

https://www.ffri.jp/research/index.htm

マルウェアに関する研究、対策技術開発

標的型攻撃など近年のマルウェア対策に関する研究成果を多数発表

独立行政法人情報処理推進機構(IPA)委託: 近年の標的型攻撃の調査研究

近年のマルウェア、脆弱性攻略手法、標的型攻撃について、いくつかの検体の全コードを網羅的にリバースエンジニアリングし挙動を分析。対策を提示。
https://www.ipa.go.jp/security/fy19/reports/sequential/index.html

国際カンファレンス、メディア等での研究成果発表多数

例:

Mac OS X を狙う新たなランサムウェアの登場
https://www.ffri.jp/assets/files/monthly_research/MR201603_The_Advent_of_New_Ransomware_Targeting_The_Mac_OS_X_JPN.pdf

不正な開発環境によるマルウェアの拡散
https://www.ffri.jp/assets/files/monthly_research/MR201601_The_diffusion_of_malware_by_malicious_development_environment_JPN.pdf

SLIME: Automated Anti-sandboxing disarmament system (Black Hat Asia)
https://www.blackhat.com/docs/asia-15/materials/asia-15-Chubachi-Slime-Automated-Anti-Sandboxing-Disarmament-System.pdf

FREEZE DRYING FOR CAPTURING ENVIRNMENT SENSITIVE MALWARE ALIVE (Black Hat Europe)
https://www.blackhat.com/docs/eu-14/materials/eu-14-Chubachi-Freeze-Drying-For-Capturing-Environment-Sensitive-Malware-Alive.pdf

TENTACLE: Envirnment Sensitive Malware Palpation (Pacsec 2014)
https://pacsec.jp/psj14/PSJ2014_chubachi_final_en.pdf

組込みセキュリティ

組込みシステムのセキュリティ脆弱性脅威分析に関する研究成果を多数発表

IPAにおける民間の組み込みセキュリティ対策推進

独立行政法人情報処理推進機構(IPA)において、民間の組み込みセキュリティ対策を推進。

経済産業省「新世代情報セキュリティ研究開発事業」

情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術研究実施。

IoTに関するセキュリティ脅威分析結果を多数発表

例:

「IoTとしての自動車とセキュリティ：リモートサービスのセキュリティ評価とその対策の検討」(CODE BLUE 2016)
https://www.ffri.jp/assets/files/research/research_papers/Security_in_the_IoT_World%EF%BC%9AAnalyzing_the_Security_of_Mobile_Apps_for_Automobiles_JP_20161110.pdf

FFRI代表・鵜飼が韓国発・セキュリティ国際会議「POC2015」で研究発表 (POC2015)
https://www.ffri.jp/assets/files/docs/1885/20151110_release.pdf

Windows 10 IoT Core に対する脅威分析と実施するべきセキュリティ対策 (CODE BLUE 2015)
https://www.ffri.jp/assets/files/research/research_papers/Threat_Analysis_on_Win10_IoT_Core_ja.pdf

「TriCoreで動作する自動車用ECUソフトの攻撃手法に関する検討と試行」 (CODE BLUE 2014)
https://www.ffri.jp/assets/files/research/research_papers/Code_Blue_Tricore_assessment_slides_ja.pdf

その他

車載システムの脅威分析、ルーター、ネットワーク機器等の脆弱性診断など多数実施。

製品・サービスラインナップ
ー法人向けー

次世代エンドポイントセキュリティ

yarai

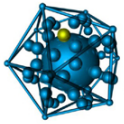
FFRI yaraiは、パターンファイルに依存しない「先読み防御」技術を徹底的に追及した次世代エンドポイントセキュリティです。 標的型攻撃のトリガーとなる未知の脆弱性攻撃や、未知のマルウェア攻撃からシステムを保護します。

標的型攻撃マルウェア検査サービス

標的型攻撃マルウェア検査サービス

標的型攻撃マルウェアの感染有無を調査。マルウェア解析を実施し、実被害を分析。対策立案や外部報告など含めた事後対応をサポート。

マルウェア自動解析ツール



yarai Analyzer
Automated Malware Analysis System

不審ファイル発見時の初動分析、ハッキングによる情報流出対策など、さまざまなマルウェア解析シーンで活用可能。

yarai Analyzer Professional
Automated Malware Analysis System

FFRI yarai analyzer Professionalは、FFRI yarai analyzerの機能に加えて、より高度な情報を自動的に抽出・レポーティングすることが可能。

製品・サービスラインナップ
ー個人・SOHO向けー

次世代エンドポイントセキュリティ

Yarai Home and Business Edition

法人向け製品「FFRI yarai」のスタンドアローン版。
独自の「先読み防御」技術により、未知のサイバー脅威に対抗する
個人・小規模事業者向け『次世代エンドポイントセキュリティ製品』。

個人向けセキュリティ対策(スマートフォン)

FFRI安心アプリチェッカー

Android用スマートフォン・タブレットでご利用になるアプリの危険性を
簡単に診断出来るセキュリティアプリ。

製品・サービスラインナップ

ー 法人向け ー

IoTデバイスのセキュリティ検査

IoTデバイス・システム　セキュリティ対策支援サービス

多数のセキュリティ脅威分析や国際的な研究成果発表実績のあるリサーチチームが、出荷前のIoTデバイスやシステムのセキュリティ脅威を分析し、対策を支援。

セキュリティコンサルティングサービス

Prime Analysis

APTマルウェア検査、Android端末セキュリティ分析、脆弱性脅威分析、パッチ解析、マルウェア解析、緊急ブリーフィングなどコンサルティングサービスを実施。

マルウェアが通信する危険なURLのリスト提供

BlackURL

独自のマルウェア収集システムによって得られたマルウェア検体から抽出した通信先の危険なURL情報の提供。

その他サービス実績

業種	カテゴリ	内容
官公庁・各種団体	受託開発	サイバー攻撃対策製品の追加機能および他OSへの移植開発
	教育・研修	マルウェア動的解析トレーニング
		マルウェア静的解析トレーニング
	調査・研究	不正プログラムの接続先解析システムの作成
		制御システムに対する脅威の検査技術に関する研究開発
情報通信	教育・研修	セキュリティ技術者育成に関する教育研修
	調査・研究	セキュリティ機構の調査・評価支援
産業インフラ・サービス	教育・研修	制御システム向けセキュリティ技術者育成支援
	調査・研究	制御システム向けマルウェア調査
		制御システムに対する脅威分析
		制御システム向けファジング手法の調査
	検査・診断	Androidアプリのセキュア開発ガイド作成支援
		ネットワーク機器のセキュリティ機能に対する検査
自動車	検査・診断	セキュア開発に関するコンサルティング
		ECUに対するテスト手法のコンサルティング
		完成車両上のIVI機器に対するペネトレーションテスト
	調査・研究	要求仕様書のアセスメント

ありがとうございました。

本講演に関する質問等お問い合わせ
norihiko.maeda@ffri.jp

FFRIセキュリティに関するお問い合わせ
https://www.ffri.jp/contact/