コミュニティ イントロ

松尾 和輝

株式会社ＦＦＲＩセキュリティ
（東証グロース：3692） https://www.ffri.jp

自己紹介 – 松尾 和輝 (@InfPCTechStack)

➢ **所属**

・FFRI セキュリティ　基礎技術研究部

➢ **研究分野**

・UEFI BIOS セキュリティ

・SMM、ハイパーバイザー、Win Kernel、(TEE や HW はかじる程度)

➢ **過去研究**

- SmmPack: Obfuscation for SMM Modules with TPM Sealed Key [DIMVA 2024]
- You've Already Been Hacked: What if There Is a Backdoor in Your UEFI OROM? [BHUSA 2024]
- Shade BIOS: Unleashing the Full Stealth of UEFI Malware [BHUSA 2025]

用語定義

Negative Ring (NR) セキュリティ

本資料では、以下に関わるセキュリティを、総称して「NRセキュリティ」と呼びます。

- BIOS (ring 0)
- ハイパーバイザー (ring -1)
- SMM (ring -2)
- CSME (ring -3)
- ハードウェア

※ Intel 以外のアーキテクチャも含む

※ Ring Minus Security の名前の由来

コミュニティ設立の背景

NR セキュリティのコミュニティが無い

- 開発であれば UEFI.org や kernel/vm 探検隊等あるが、セキュリティに特化しているわけではない
- 3mdeb、FOSDEM、OSFC が近いが、closed なファームウェアを open にしていこうという思想
  => 設計から変えよう ではなく、今ある PC の NR 攻撃/防御について議論できる場が無い
- OEM 等は NDA で情報が閉じており、セキュリティコミュニティにあまり顔を出さず、交流が難しい
- 非特化型の国内/国際学会/カンファレンスでは分野外の方が多く、深い議論はあまり期待できない

その結果、

- NR セキュリティの重要性が普及していない
  - 例えば、ブートキットがどう感染するのか等の前提もほとんどの人は知らない
- NR セキュリティの知見が分散している
  - NR セキュリティの対策をしたくても、どこを参考に/どこに聞けばいいかわからない状況
- NR セキュリティをビジネスに活かせるルートがない
  - NR セキュリティ周りの取り組みは趣味として完結して活かされてない物が多い印象
- そもそも圧倒的にツールや研究が不足している

コミュニティの趣旨

NR セキュリティを広める

- NR セキュリティがどう大事なのか、どう被害に繋がるのかを周知して解像度を上げる
- NR セキュリティの知見を集約して、本コミュニティを見れば対策方法などわかるようにする
- NR セキュリティの研究やツールを増やし、発表できる場を増やす
- NR セキュリティの研究をビジネスに還元したり、OEM 側との交流できる環境を整える
- NR セキュリティに携わる技術の情報交流を促進する

まとまったコミュニティができ、定期的に周知していれば他色んな機会にも繋がると思います

コミュニティの詳細

参加者

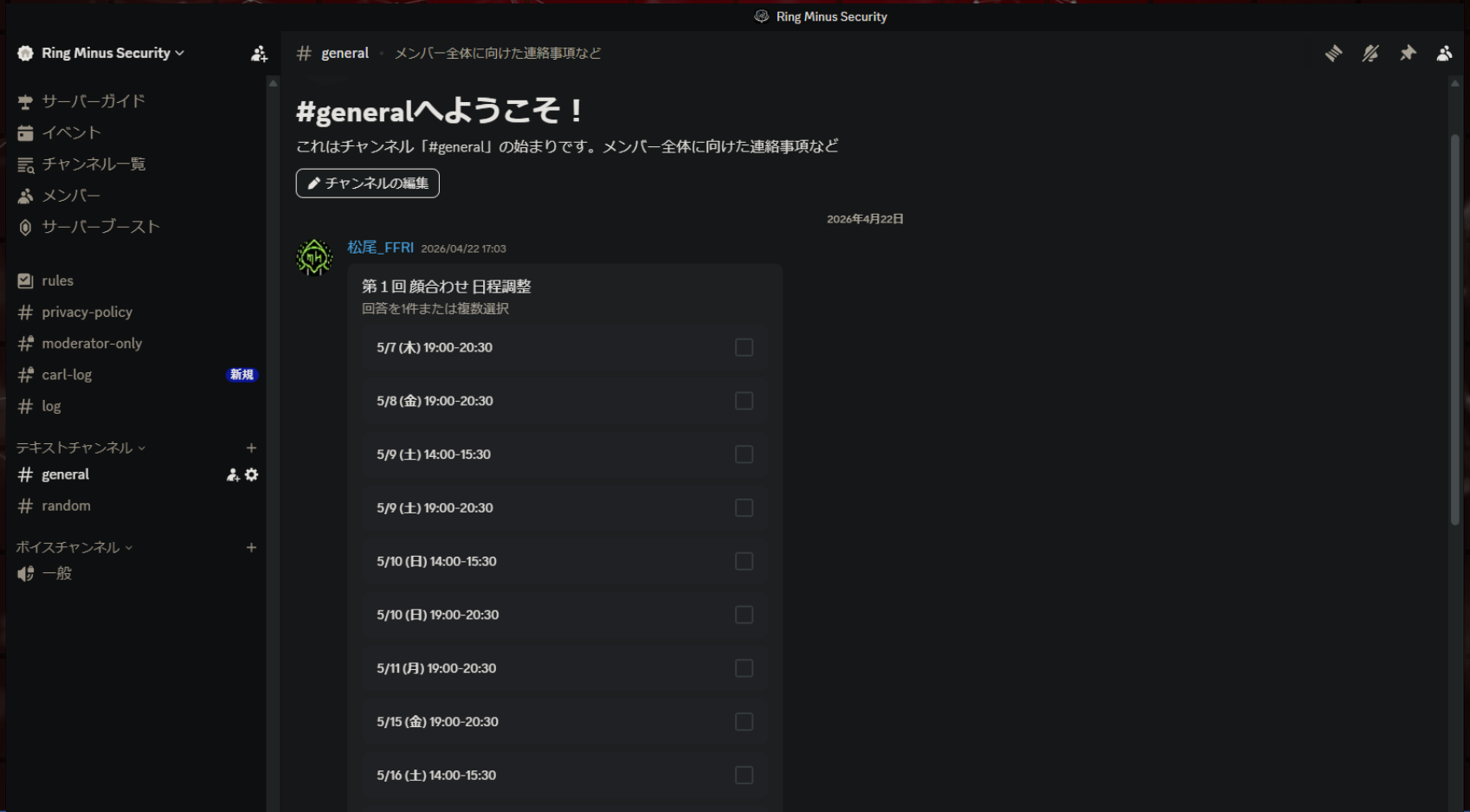
- 国内外で NR セキュリティを研究/実務で扱っている方全般
- BIOS ベンダー、OEM、シリコンベンダー
- 企業や政府機関で PC の調達に関わる方
- NR セキュリティに興味がある方

活動内容（案）

- 勉強会/LT会
- ブログや動画等の掲載による周知
- 整理された外部ブログのリンク集
- オフサイトイベントや Discord での交流
- 共同研究/開発 – カンファレンスでの発表
- 本の執筆
- セキュキャンやカンファレンスへのブース提供、カンファレンス開催
- マルウェア解析レポート、高度な攻撃の解説...

※ 関わり方は自由で、これらを強制するわけではありません

コミュニティ内での交流 - Discord

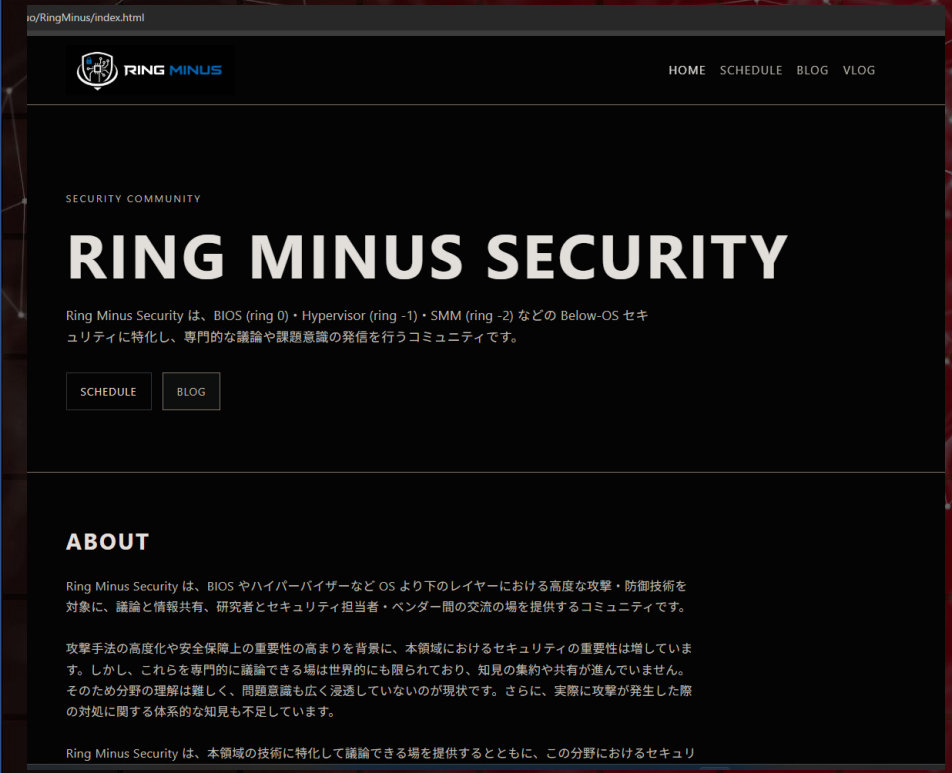


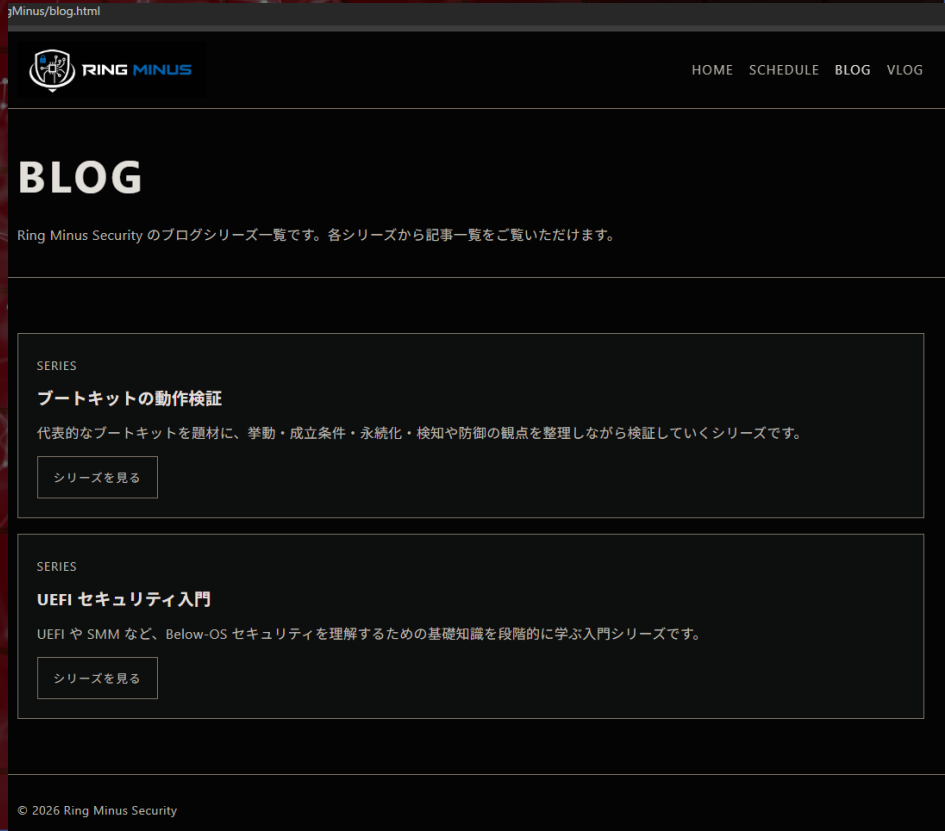
コミュニティによる周知 - X

コミュニティによる周知 – ホームページ

勉強会の開催日や、ブログ掲載、コミュニティの趣旨や応募フォーム等

https://ffri.github.io/RingMinus/





コミュニティ参加者のメリット

NR セキュリティの情報共有ができる

- 一人で研究してわからない所などをコミュニティ内で質問できる
- 特に低レイヤーは複数の PC/機器 が検証に必要などとコストが高いが、お互い協力し合える

NR セキュリティの取り組みを周知できる

- 開発したツールやカンファレンス登壇などの宣伝を周知したり、勉強会で発表できる

NR セキュリティの取り組みをビジネスに還元しやすい環境が得られる

- NR セキュリティに携わるセキュリティ関係者は、OEM 等のベンダーがいる場で自分の取り組みを直接伝えられる
- ベンダー側は、製品に載っている詳しい NR セキュリティの技術内容を分野に興味がある方へ周知できる

とはいえ、何より楽しく、柔軟に活動できれば！