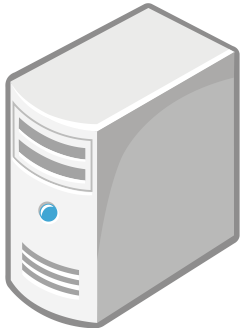
セキュリティベンダーが安心をご提供
ＦＦＲＩセキュリティ マネージド・サービス

ＦＦＲＩセキュリティ ウェビナー
2022年7月22日 オンラインLive配信

株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp

昨今の攻撃トレンド

- Attack Vectorの切り口で考えてみる



どこまで守れるのか

- 守るべき情報資産は、どこに格納されているか
- 一般的には散在しているはず
  - (例) 社内ネットワークに設置しているファイルサーバー
  - (例) 各PC端末（エンドポイント）
  - (例) クラウドサービス上
- 資産管理の重要性
- バックアップの重要性

- エンドポイント保護の重要性

- とは言え、もし攻撃されてマルウェアが発動したら・・・

Why FFRI yarai ?

FFRI yarai Cloud

FFRI yaraiの管理サーバーをクラウド環境でご提供
サーバー導入／運用管理を省力化可能です

振る舞い検知型マルウェア対策
(先読み技術)

マルウェア特有の
怪しい振る舞いなどの特徴を判断

パターンファイルに依存しない
振る舞い検知で未知のマルウェアも防御

管理サーバー不要

Windowsライセンス、
サーバー費用、スペース、
設備費用、サーバー管理等が
不要になり**コスト削減**

更新作業の削減

管理コンソールの更新作業は
ＦＦＲＩセキュリティ側で実施
バージョンアップ作業の
時間と工数が削減

クライアント一元管理

クライアントが
他拠点に分散していたり
外出先／出張先／在宅勤務でも
インターネット経由で一元管理

シンプルな管理画面

管理コンソールはシンプルな
操作でご利用いただけます。
もちろん**日本語表示**でお使い
いただけます。

yarai 3.5.0 主な新機能

- 検出エンジン強化
  - Office マクロの静的検出機能追加
  - 機械学習エンジンの機能強化
- 検出マルウェアの可視化機能
- 管理機能強化
  - FFRI AMC の外部連携機能の強化（syslog）
  - マルチテナントの運用機能の強化
  - 新 OS サポート

FFRI yarai マルウェア検出速報

- https://www.ffri.jp/products/yarai/defense_list.htm

2022/06/17公開

Black Basta

ハッシュ値(SHA-256)	5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa
エンジン	Static分析エンジン
検証環境	Windows10 × FFRI yarai 3.2.4(2019年1月リリース)
関連情報	新種ランサムウェア「Black Basta」の感染活動を分析、QAKBOTやContiとの関連性とは

2022/06/14公開

RobinHood

ハッシュ値(SHA-256)	f9533288e6a7279195902c8691d5f223c77015fa332b56e23aeec3581c0cdbdb
エンジン	HIPSエンジン
検証環境	Windows10 × FFRI yarai 3.2.4(2019年1月リリース)
関連情報	【独自】トヨタ工場の停止、ハッカー集団「ロビンフッド」関与…未確認ウイルスのため即復旧を断念
関連ブログ	【追加更新】経営課題としてサイバー脅威への認識を

2022/06/15公開

Emotet(2022年6月版)

ハッシュ値(SHA-256)	33c838d83a06db3364009cf58d2de073ffa732e1d4401f6ad7832e309e225292
エンジン	HIPSエンジン
検証環境	Windows10 × FFRI yarai 3.4.3 (2021年5月リリース)
関連情報	Emotetの解析結果について
関連ブログ	Emotetの感染が再び増えています

2022/05/12公開

Emotet(2022年5月版)

ハッシュ値(SHA-256)	a10a61bf2969fe0c40741a28a3f79125ece10be7dab90f1095bb7095c47b168c
エンジン	HIPSエンジン
検証環境	Windows10 × FFRI yarai 3.4.3 (2021年5月リリース)
関連情報	マルウェアEmotetの感染再拡大に関する注意喚起
関連ブログ	Emotetの感染が再び増えています

100%防げる・守れる製品

- おそらくこの世に存在しない
  - ホワイトリスト適用ができる環境であれば、100%は達成し得る可能性
  - ただし、稀

- 「万が一マルウェア感染が起きてしまった場合」を想定
  - 訓練
  - 体制
  - 運用・監視
  - 感染が起きたときの初動対応（インシデントレスポンス）

ＦＦＲＩセキュリティ マネージド・サービス

サイバーセキュリティ対策の課題

- ✓高度なサイバーセキュリティ対策を行うと運用に負担がかかってしまう
- ✓サイバーセキュリティの専門的な人材を雇用するのは難しい
- ✓サイバー攻撃を受けていても認識できないかもしれない
- ✓インシデントが起きた時にどうすれば良いかわからない

“サイバーセキュリティの専門企業”
ＦＦＲＩセキュリティのマネージド・サービスで解決します！

ＦＦＲＩセキュリティ　マネージド・サービス

1.アラートモニタリングサービス

2.インシデント初動調査サービス

3.レポートサービス

4.製品サポート

＋ yarai

運用支援サービスとFFRI yarai でセキュリティ対策のお悩みを解決します

※本サービスにて利用するFFRI yaraiは「FMS用FFRI yarai」です

アラートモニタリングサービス

アラートモニタリング

■ セキュリティアナリストがモニタリングを行い、インシデントの可能性がある場合にはご連絡や端末隔離などの対応をいたします。

例外リスト対応支援

■ 運用支援のため例外リストの設定方法に関するご支援もいたします。

クライアント稼働状況確認

■ バージョンアップ状況やクライアントの稼働状況のモニタリングを行い必要に応じた運用支援を行います。

インシデント初動調査サービス

インシデント初動調査

■ マルウェアの感染など、インシデントの発生が疑われる場合には**初動対応**に関するご相談を承ります。

マルウェアハンティング

■ マルウェアの検出があった場合には他の端末に存在がないかを調査することが可能です。

インシデント簡易調査

■ 必要に応じて不審なプロセスのチェックや簡易マルウェア分析といった対応が可能です。

※復旧やインシデントクローズに向けたインシデントハンドリングのご支援が必要となった場合には別途オプションにて「インシデントハンドリング支援サービス」のご提供が可能です。

レポートサービス/製品サポート

レポートサービス

- 検出状況やインシデントの発生状況、FFRI yaraiの稼働状況などを月次レポートにてご連絡いたします。
- サイバーセキュリティに関するトピックを不定期にてご提供いたします。

製品サポート

- FFRI yarai cloudに関する製品トラブルも当サービスにてご対応いたします。メーカーサポートのため安心してご利用いただけます。

導入支援作業

サービスの導入に伴い、FFRI yarai cloudの導入もご支援いたします。

【作業例】
- 運用ポリシー設計
- ライセンスの配布設定
- ポリシーの配布設定
- 例外リストの作成及び配布

※別途有償での作業となります。費用についてはお問い合わせください。

FMS用 FFRI yarai

FFRI yaraiの管理サーバーをクラウド環境にてご提供いたします。
サーバー導入／運用管理を省力化します。

振る舞い検知型マルウェア対策
(先読み技術)

マルウェア特有の
怪しい振る舞いなどの特徴を判断

パターンファイルに依存しない
振る舞い検知で未知のマルウェアも防御

管理サーバー不要

Windowsライセンス、
サーバー費用、スペース、
設備費用、サーバー管理等が
不要になり**コスト削減**

更新作業の削減

管理コンソールの更新作業は
ＦＦＲＩセキュリティ側で実施
バージョンアップ作業の
時間と工数が削減

クライアント一元管理

クライアントが
他拠点に分散していたり
外出先／出張先／在宅勤務でも
インターネット経由で一元管理

シンプルな管理画面

管理コンソールはシンプルな
操作でご利用いただけます。
もちろん**日本語表示**でお使い
いただけます。

サービスイメージ

端末アクティビティの監視に加え、セキュリティアナリストによるモニタリング、調査、レポートサービスなどの高度なサイバーセキュリティ対策をご提供します。

検知

- **FFRI yarai** が端末内のアクティビティをリアルタイムで監視、サイバー攻撃による不審なふるまいを検知します。

モニタリング

- セキュリティアナリストが**アラートモニタリング**を実施。
- インシデントの可能性がある場合にご連絡や端末隔離などの対応をいたします。

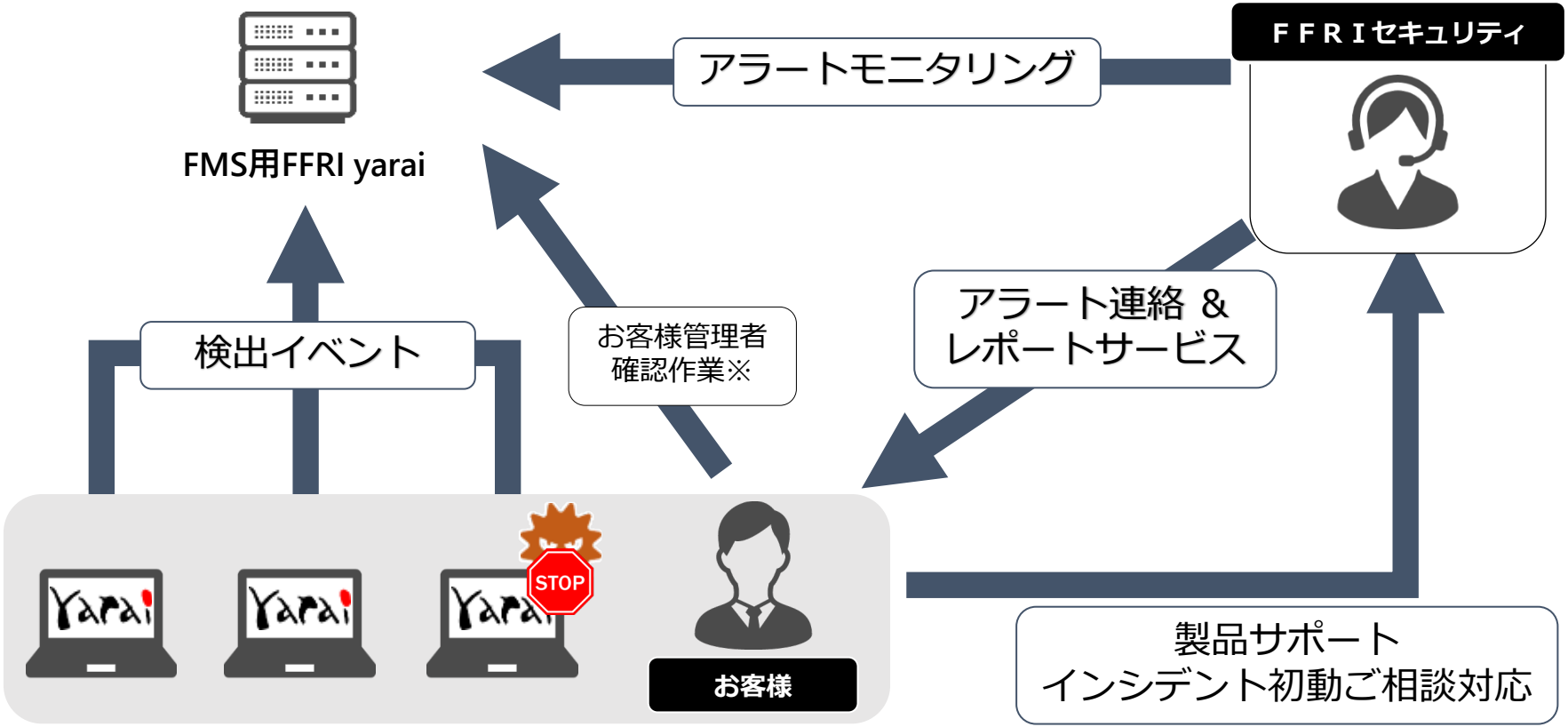
調査

- インシデントの発生が疑われる場合には**インシデント初動調査サービス**にて初動対応をご相談いただくことができます。

レポート

- **レポートサービス**にて検出状況やインシデントの発生状況、yaraiの稼働状況などを月次にてレポートいたします。

サービスイメージ



※例外リスト対応チューニング、バージョンアップ作業、ユーザヒアリングなど

オールインワンパッケージ

ＦＦＲＩセキュリティ マネージド・サービスは次世代エンドポイントセキュリティである FFRI yarai cloudにマネージドサービス、製品サポートがオールインワンとなり、お客様のサイバーセキュリティに関するお悩みを解決します。

FFRIセキュリティ マネージド・サービス

- FFRI yarai cloud
- アラート モニタリング サービス
- インシデント 初動調査 サービス
- レポート サービス
- 製品サポート

FFRI yaraiとＦＦＲＩセキュリティによるマネージドサービスがオールインワン

サービス内容一覧

項目	機能
エンドポイント保護	振る舞い検知
	クラウド連携
	検体自動判定
	Microsoft Defender連携
監視サービス	アラートモニタリング
運用支援	製品サポート
	例外リスト対応支援
	クライアント稼働状況確認
	レポートサービス
	サイバーセキュリティ情報配信
インシデント対応	端末隔離
	インシデント初動調査
	マルウェアハンティング
	インシデント簡易調査
	インシデントハンドリング支援 ※別途オプション

ありがとうございました