SKYSEA Client View

組織の重要データを守るために、セキュリティ対策はできていますか？

SKYSEA Client View EDRプラスパックのご紹介

インターネットに接続しなくても使える「EDR」

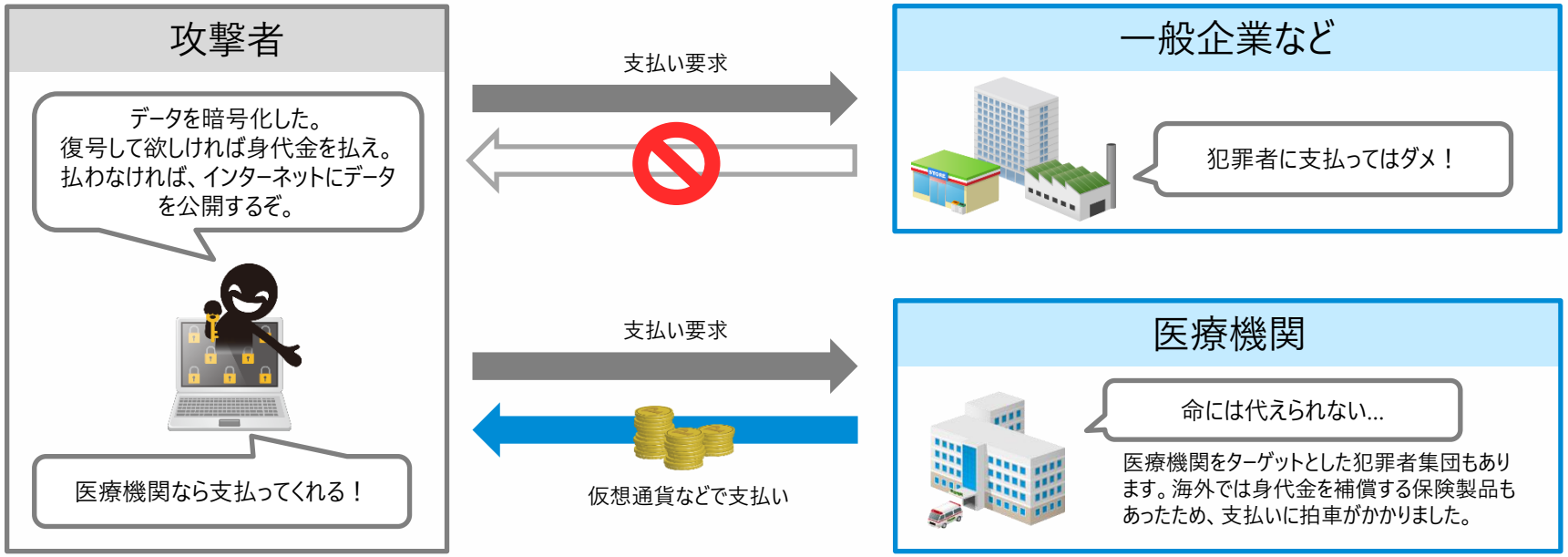
Sky

医療機関を狙うサイバー攻撃

データを暗号化して身代金を要求する「ランサムウェア」が問題になっています。

ランサムウェアに感染してデータが暗号化された場合、犯罪者集団の資金源になってしまうため、一般的には「身代金を支払ってはいけない」と言われています。

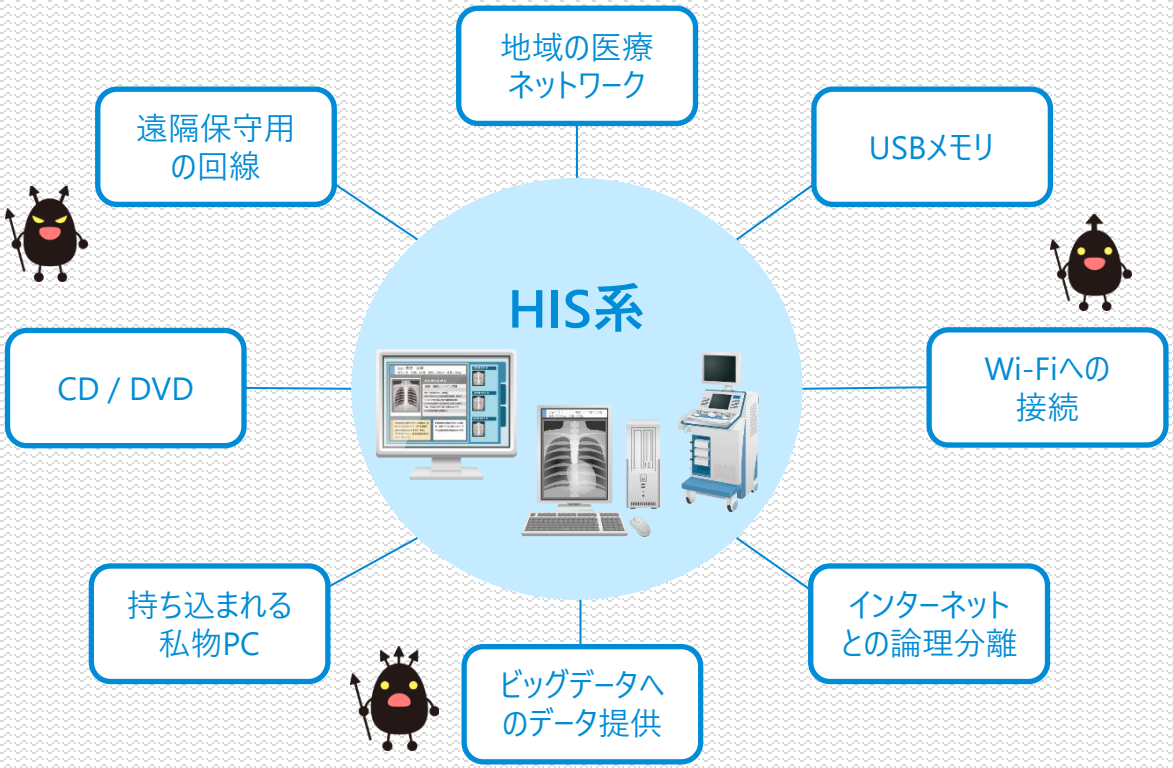
しかし病院の場合、診療データが使えないと命に係わるため、特に海外で身代金が支払われた事例があります。その結果、犯罪者集団に狙われやすくなってしまっています。



医療機関は海外で身代金の支払い事例があり、犯罪者集団に狙われやすいです。

「インターネットから分離されているので安心」ですか？

電子カルテなどのHIS系ネットワークは、インターネットから分離されているので安心と思われがちです。ところが医療の質を高めるための情報化や、地域医療連携などの取り組みの結果、従来のUSBメモリに限らず、様々な経路からランサムウェアなどへの感染が報告されています。

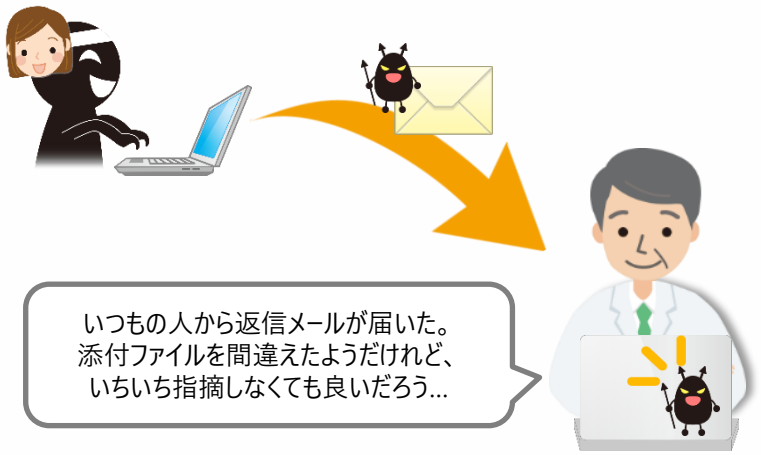


1ヶ所でも情報セキュリティ対策が不十分だと、侵入されるリスクがあります。

巧妙なサイバー攻撃

コンピュータにランサムウェアを感染させる方法は、大きく分けて2種類あります。いずれの手法も、高度で巧妙なものになりつつあるため、完全に防ぐことは困難と考えられるようになりました。

A：不正プログラムに感染させる



B：システムの脆弱性から侵入する

侵入されても、被害が発生する前に防ぐ取り組みが求められています。
特に不正プログラム対策については、令和3年（2021年）7月7日に「政府機関等の対策基準策定のためのガイドライン」の改定で、対策の強化が求められています。

医療情報システムの安全管理に関するガイドライン

2022年3月、医療DXへの取り組みや、相次ぐ病院へのサイバー攻撃を踏まえて第5.2版への改定が行われました。未知の不正ソフトウェアへの対策として、**「EDR」や「ふるまい検知」が有効**とされています。

6.5. 技術的安全対策　B.　考え方　(5)不正ソフトウェア対策

出典：医療情報システムの安全管理に関するガイドライン第5.2版
https://www.mhlw.go.jp/content/10808000/000884640.pdf

コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正ソフトウェア（以下「不正ソフトウェア」という。）は、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に入る可能性がある。不正ソフトウェアの侵入に際して適切な保護対策が行われていなければ、セキュリティ機構の破壊、システムダウン、情報の漏えいや改ざん、情報の破壊、資源の不正使用等の重大な問題が引き起こされる。そして、何らかの問題が発生して初めて、不正ソフトウェアの侵入に気付くことになる。

対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が最も効果的でると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できる。また、このことは医療機関等の外部で利用する端末やPC等についても同様であるが、その考え方と対策については、6.9章を参照すること。

ただし、これらの不正ソフトウェアは常に変化しているため、検出するためのパターンファイルや検索エンジンを常に最新のものに更新しておく必要がある。また、たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、医療情報システム側の脆弱性を可能な限り小さくしておくことが重要である。そのために実施すべき対策として、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの非活性化、マクロ等の利用停止、メールやファイルの無害化がある。また、**EDR（Endpoint Detection and Response）や「振る舞い検知」などの方策も有効である**。なお、いずれの対策を行う場合も、対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要である。

本ご提案書では、「EDR」と「ふるまい検知」の両方の特性を兼ね備えた、「SKYSEA Client View EDRプラスパック」をご案内いたします。

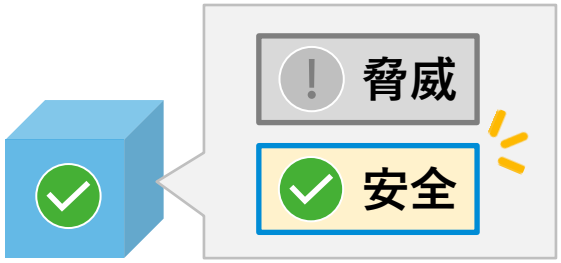
EDR （Endpoint Detection and Response）とは

EDRは「サイバー攻撃の発見」から「対処する」までを対象とするソフトウェアです。
サイバー攻撃の全体を可視化し、原因究明・影響範囲の特定に活用できる以下の4機能が求められます。

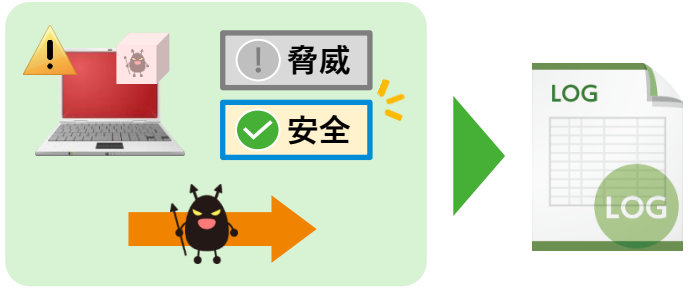
① 検知ファイルの収集・隔離

② 検知ファイルの他端末での存在調査・隔離

③ 隔離ファイルの復旧



④ ログの収集



EDRプラスパックは、SKYSEA Client ViewとFFRI yaraiとの連携を強化し、これらの機能をご提供します。

SKYSEA Client View EDRプラスパックとは

新オプション『SKYSEA Client View EDRプラスパック』は、エンドポイントにおける不審な挙動を検知し、迅速な対応を支援します。「SKYSEA Client View」によるファイル操作などのログ収集・管理機能と「FFRI yarai」による、ふるまい検知・防御の機能の連携をより強化させて提供いたします。

SKYSEA Client View EDRプラスパック

SKYSEA Client View

クライアント運用管理ソフトウェア

ファイル操作などのログ取得による調査

＋

Yarai

次世代エンドポイントセキュリティ

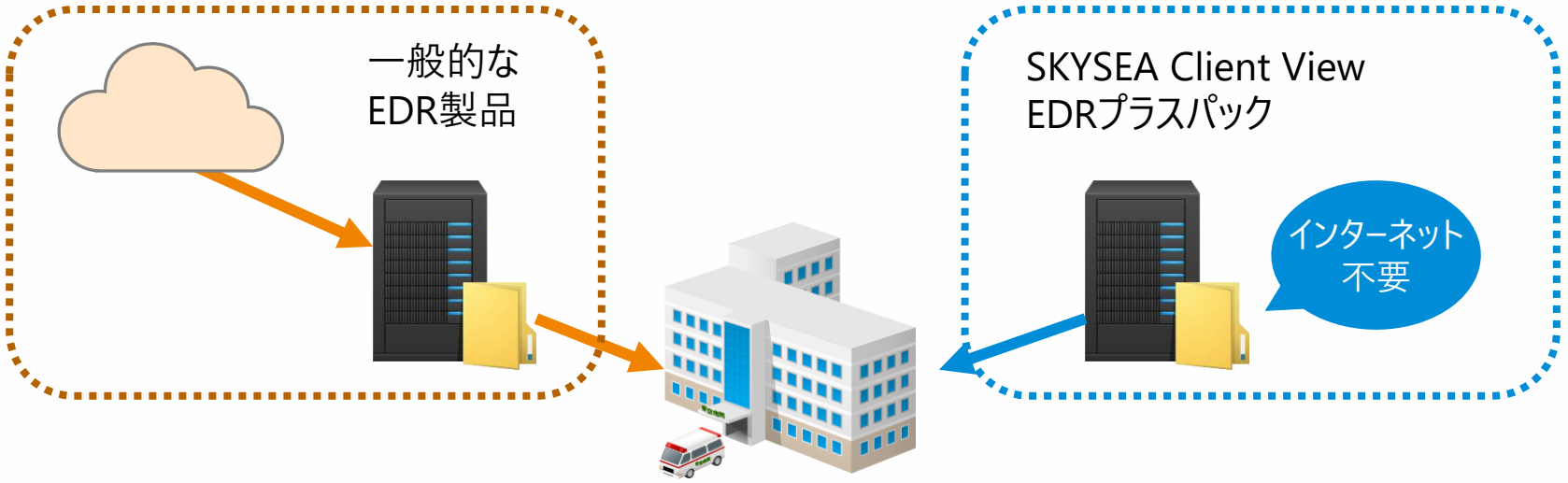
ファイルの特徴や実行プロセスのふるまいを
監視して検知・防御

**SKYSEA Client View と FFRI yaraiを組み合わせることで、
サイバー攻撃などのエンドポイント対策を支援します！**

特長① HIS系でご利用可能

一般的なEDR製品はインターネット接続が必要です。そのため、HIS系ネットワークでのご利用が難しいです。
一方、SKYSEA Client ViewのEDRプラスパックは、オンプレミス環境で運用できるのが特長です。

※クラウド環境でのご利用も可能です。



**SKYSEA Client View EDRプラスパックは
インターネット接続環境のない、HIS系でもご利用可能です。**

特長② 発症する前に防御し、感染源を調査可能

一般的なEDR製品は、情報の持ち出しなどを検知して対応を始めます。
一方、SKYSEA Client ViewのEDRプラスパックは、不正プログラム特有のふるまいから検知し、防御します。
また、影響範囲や感染経路の調査を行うことで、再感染の防止を支援します。

既知のマルウェアを検知

AV Antivirus。
EPP（Endpoint Protection Platform）とも呼ばれる

パターンファイルによるマルウェア検知

イメージ

未知のマルウェアも検知

NGAV Next Generation Antivirus

マルウェア特有の動作を基に検知

イメージ

端末の動きをもとに検知

一般的な **EDR** Endpoint Detection and Response

エンドポイントの動きを基に検知

イメージ

SKYSEA Client View EDRプラスパックは
「ふるまい検知」で、発症前の防御を行いつつ、再感染の防止も支援します。

FFRI yaraiについて

次世代エンドポイントセキュリティ「FFRI yarai」のご紹介

2009年にパターンマッチング技術に依存しない完全ふるまい検知製品として販売開始以来、
純国産のエンドポイント型未知の脅威対策製品として高い評価を得ています。

先読み技術

パターンファイルに依存しない
ふるまい検知で
未知の脅威を防御！

高い防御力

洗練された
5つのエンジンで
未知の脅威を防御！

豊富な導入実績

官公庁や地方自治体で
導入実績多数！

安心の純国産

基礎技術研究から
開発・保守に至る全工程を
日本国内で実施！

先読み技術で未知の脅威から防御

従来のパターンマッチングベースでは検知が困難な未知のマルウェアや脆弱性攻撃を、FFRI yaraiの先読み技術を用いた「ふるまい検知」により防御します。

パターンマッチング型

定義ファイルを用いたパターンマッチングにより
既知のマルウェアを検知

パターンファイルに登録されていないと
未知のマルウェアは防げない

ふるまい検知型

FFRI yarai

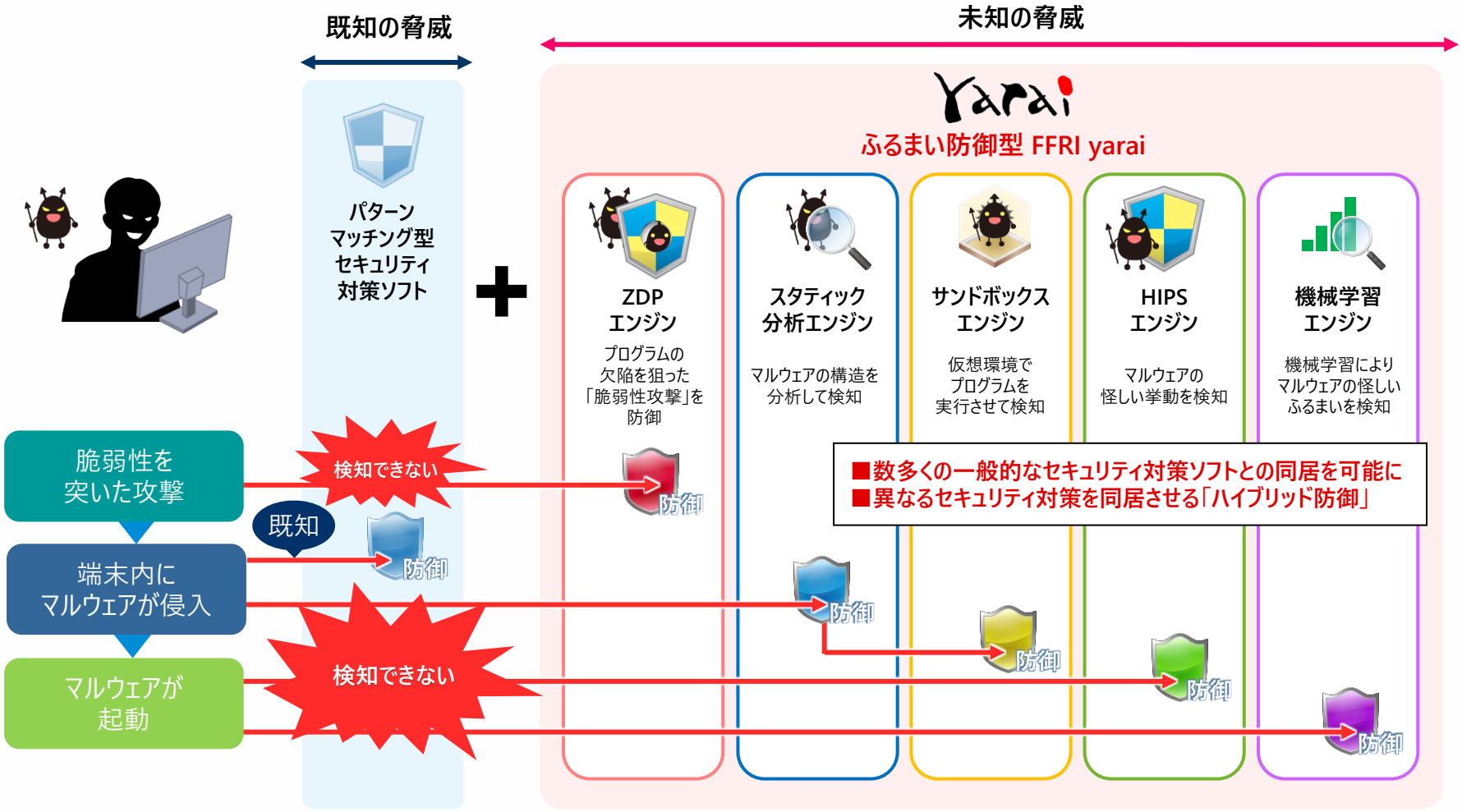
マルウェア特有の
怪しい「ふるまい」などの特徴を検知

パターンファイルに依存しない
ふるまい検知で未知のマルウェアも防御

EmotetやLockBit 2.0も検出実績があります

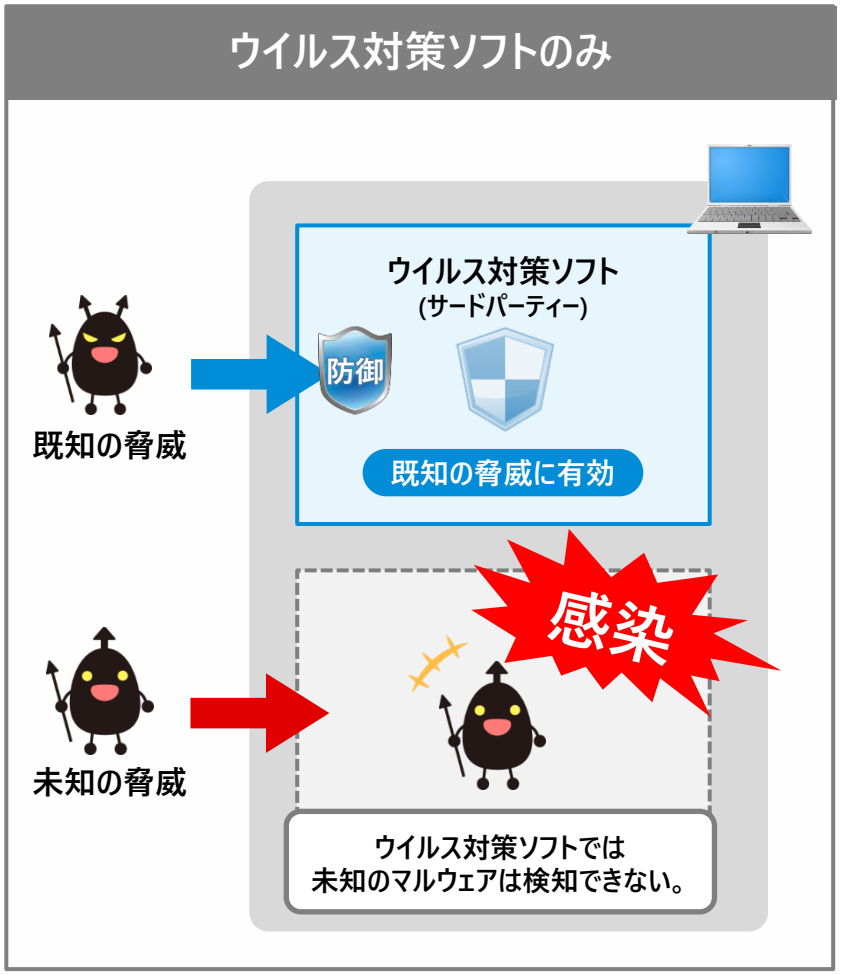
エンドポイントでハイブリッド防御-1

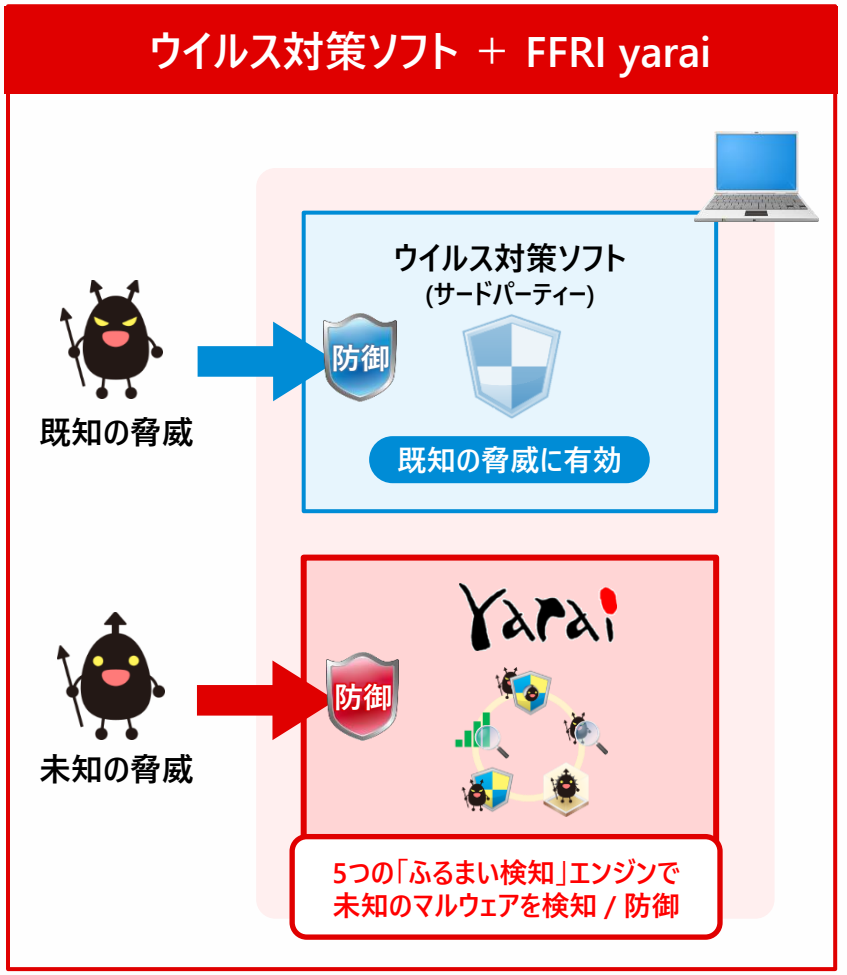
一つのエンジンで検知できなかったとしても他のエンジンがカバー。多層防御で幅広いタイプのマルウェアに対応しています。既存対策と組み合わせることで、未知の脅威への防御力が大幅に向上します。



エンドポイントでハイブリッド防御-2

ウイルス対策ソフトとFFRI yaraiを連携させたハイブリッド防御は、防御範囲を拡大し、マルウェアを検知 / 防御します。





何故ハイブリッド防御での運用が必要？

「パターンマッチング型マルウェア対策」と「ふるまい検知型マルウェア対策」では、検知の仕方が違います。

パターンマッチング型マルウェア対策

マルウェア等の侵入については、
ふるまい検知型より、マルウェアの種類や数が多く、古くからある既知の脅威性に対する防御や検知が得意です。

迷惑メール

迷惑をかけるマルウェア

ふるまい検知型マルウェア対策（FFRI yarai）

未知・既知問わず、マルウェアが情報を抜き取ったり、データ破壊など脅威性に対する防御や検知が得意です。

情報を抜き取り

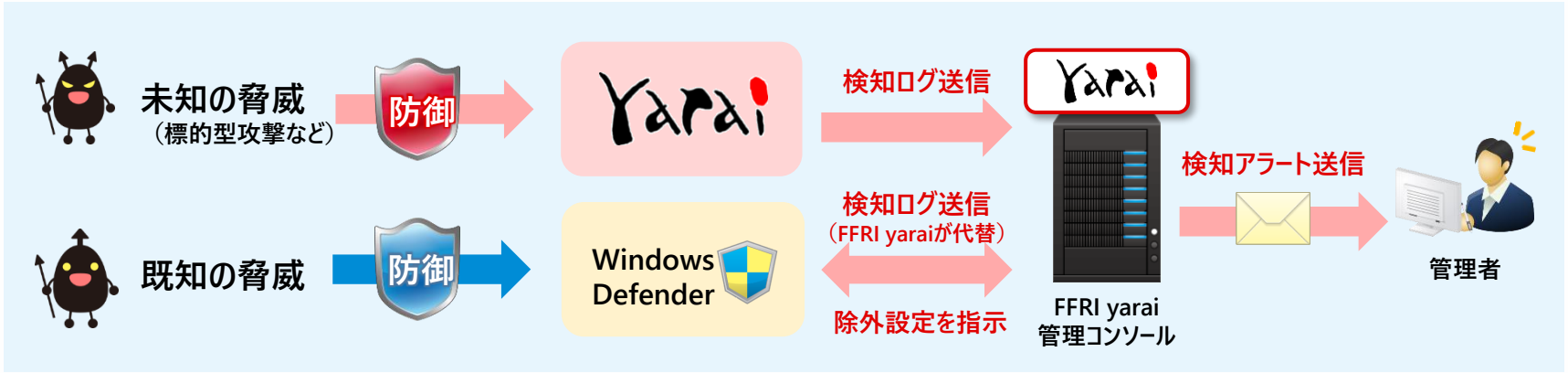
データ破壊

「パターンマッチング型」「ふるまい検知型」を併用したマルウェア対策をお勧めします。

Windows Defenderとの連携について

Windowsには無料のウイルス対策機能「Windows Defender」が付属しておりますが、管理機能を持っておりません。ステータス管理やアラート管理、除外設定管理など一元管理するためには、「Windows Defender ATP」や「Microsoft Intune」などと併用運用する必要があり、導入には構築や運用に専門の知識や技術が必要となります。しかし、FFRI yaraiではWindows Defenderの管理機能をもっており、FFRI yaraiの管理機からWindows Defenderの運用を一括で管理し、運用にかかる負荷やコストを軽減します。

FFRI yaraiを導入



FFRI yaraiの防御実績（未知のマルウェア）

FFRI yaraiは、被害発生以前にリリースされた防御エンジンで、未知のマルウェアを排除します。

発生/報道時期	防御エンジンリリース時期	当時の未知脅威及び標的型攻撃	FFRI yarai 検知&防御エンジン
2020年7月	2018年2月	ランサムウェア「Maze」	Static分析エンジン
2020年7月	2018年2月	マルウェア「Emotet」(2020年7月版)	HIPSエンジン
2019年1月	2018年3月	ランサムウェア「Anatova」	HIPSエンジン
2018年8月	2018年3月	Windowsタスクスケジューラを利用したマルウェア	Static分析エンジン
2018年7月	2018年3月	マルウェア「Emotet」(2018年版)	Sandboxエンジン
2018年4月	2017年6月	ランサムウェア「Satan」	Static分析エンジン
2018年4月	2017年6月	ランサムウェア「GandCrab」	HIPSエンジン
2018年3月	2017年6月	バンキングマルウェア「Panda Banker」	HIPSエンジン
2018年1月	2017年5月	ランサムウェア「SpriteCoin」	HIPSエンジン
2018年1月	2017年5月	ランサムウェア「Rapid」	Static分析エンジン
2017年12月	2017年5月	仮想通貨採掘マルウェア「CoinMiner」	HIPSエンジン
2017年12月	2017年5月	「楽天カード株式会社」を装ったマルウェア	HIPSエンジン
2017年8月	2016年10月	国内防衛産業を標的としたマルウェア	Static分析エンジン
2017年5月	2016年10月	ランサムウェア「WannaCry/WannaCrypt」	Static分析エンジン
2017年1月	2016年9月	IoTマルウェア「Mirai」	Static分析エンジン
2015年6月	2014年8月	日本年金機構を狙うマルウェア「Emdivi」	（非公開）

当時の未知の脅威及び標的型攻撃の発生時期より、およそ1ヶ月から1年程前に防御エンジンをリリース

※FFRI yaraiの防御エンジンリリース時期は、当時の未知脅威及び標的型攻撃の発生時期より、およそ1ヶ月から1年程前のものであり、脅威が発生する以前の防御エンジンにより防御が可能であったことを示しています。
※防御実績はFFRIセキュリティ社内で入手、検証を行った検体に関する結果であり、全ての亜種の検知を保証するものではございません。

FFRI yaraiの防御実績（0-day脆弱性攻撃）

FFRI yaraiは、被害発生以前にリリースされた防御エンジンで、0-day脆弱性攻撃を排除します。

発生/報道時期	防御エンジンリリース時期	当時の未知脅威及び標的型攻撃	FFRI yarai 検知&防御エンジン
2018年5月	2017年12月	VBScriptの脆弱性(CVE-2018-8174)	ZDPエンジン
2018年5月	2017年12月	Adobe Acrobat / Adobe Readerの脆弱性 (CVE-2018-4990)	ZDPエンジン
2018年1月	2017年6月	Adobe Flash Playerの脆弱性(CVE-2018-4878)	ZDPエンジン
2017年1月	2015年7月	Firefoxの脆弱性(CVE-2017-5375)	ZDPエンジン
2015年7月	2013年11月	Adobe Flash Playerの脆弱性 (CVE-2015-5119 / CVE-2015-5122)	ZDPエンジン
2015年6月	2013年11月	Adobe Flash Playerの脆弱性(CVE-2015-3113)	ZDPエンジン
2015年1月	2014年12月	Adobe Flash Playerの脆弱性(CVE-2015-0311)	ZDPエンジン
2014年11月	2014年8月	一太郎の0-day脆弱性(CVE-2014-7247)	ZDPエンジン
2014年2月	2013年11月	IEの0-day脆弱性(CVE-2014-0322)	ZDPエンジン

当時の未知の脅威及び標的型攻撃の発生時期より、およそ2ヶ月から1年8ヶ月程前に防御エンジンをリリース

※FFRI yaraiの防御エンジンリリース時期は、当時の未知脅威及び標的型攻撃の発生時期より、およそ2ヶ月から1年8ヶ月程前のものであり、脅威が発生する以前の防御エンジンにより防御が可能であったことを示しています。

SKYSEA Client View
EDRプラスパックについて

Sky株式会社

「EDRプラスパック」と「ITセキュリティ対策強化」の違いについて

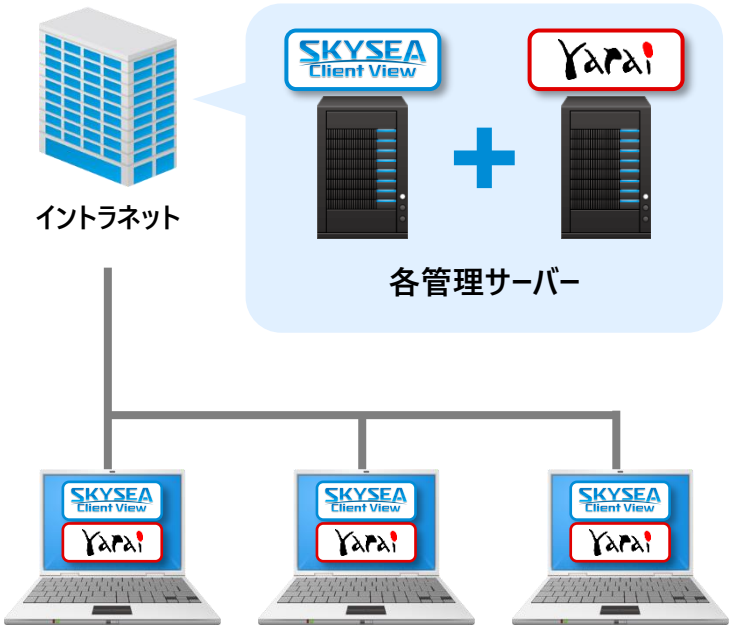
	EDRプラスパック	ITセキュリティ対策強化オプション
FFRI yaraiが異常を検知すると SKYSEA Client Viewが該当の端末をネットワークから遮断	●	●
検知・遮断された結果を管理機のログ管理画面で確認	●	●
検知したマルウェアの保存先のフルパスをログに追加	●	×
マルウェアの保存先のログを基準にしたファイル追跡機能	●	×
検知ファイルの収集・隔離	●	×
検知ファイルの他端末での存在調査・隔離	●	×
検知ファイルの復旧	●	×
検知ファイルの情報、収集した検知ファイルの情報、復旧したファイルの情報を管理機のログ管理画面で確認	●	×

※EDRプラスパックは「FFRI yaraiのライセンス」と「FFRI yarai連携ログ強化ライセンス」が含まれています。
※EDRプラスパックは「ITセキュリティ対策強化オプション」をお持ちでなくてもご利用いただけます。

EDRプラスパックの運用イメージ

オンプレミス環境の場合

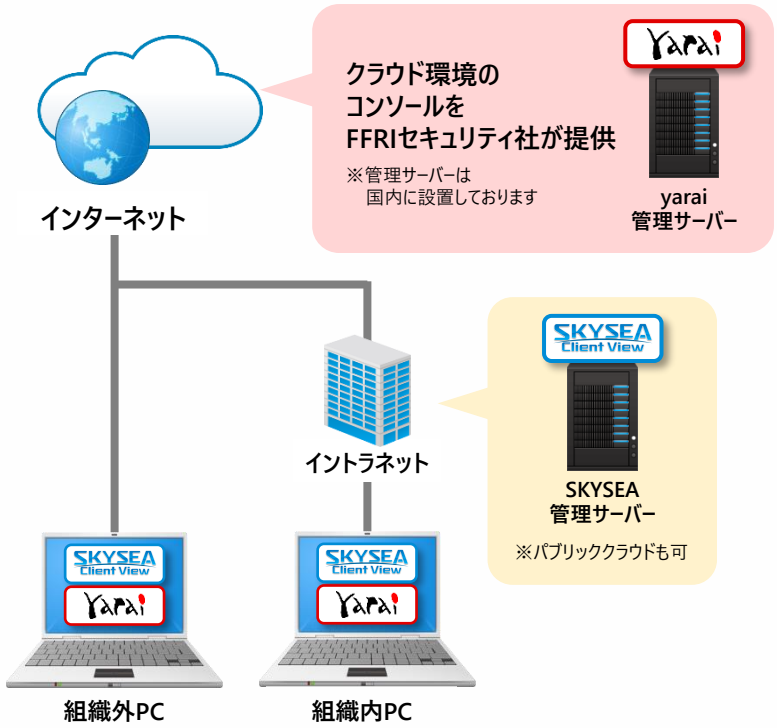
EDRプラスパック



- インターネットから分離した環境に導入したい
- クラウド上での情報管理に抵抗がある
- 組織内でサーバーを管理したい

クラウド環境の場合

EDRプラスパック Cloud



- 管理サーバーの導入コストや運用 / 更新コストを削減したい
- 管理サーバーのバージョンアップ作業が不要
- 拠点PCや外出先PCも管理したい

異常端末を検知、ネットワークから遮断

FFRI yaraiでマルウェアを検出・防御した際に出力される情報を元にし、SKYSEA Client Viewが対象のPCをネットワークから自動的に遮断することで、二次被害・拡大防止にお役立ていただけます。またネットワークを遮断した後も、SKYSEA Client View との通信は維持することができます。

マルウェアを検出/駆除

FFRI yaraiが
マルウェアを検出 / 駆除

イベントログの検出

SKYSEA Client Viewが
FFRI yaraiの出した
イベントログを検出

自動でネットワークを遮断

SKYSEA Client Viewが
自動で
ネットワークを遮断

PCの安全を確認

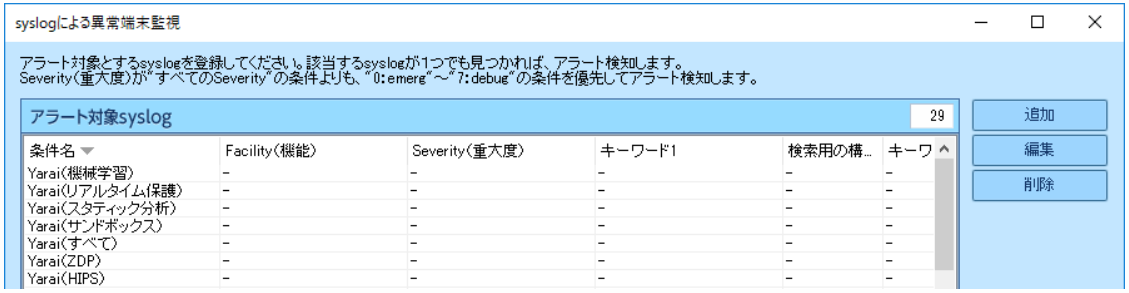
ネットワーク遮断の解除

SKYSEA Client Viewが
遮断を解除

FFRI yaraiがマルウェアを検出したときのsyslogログをアラート対象として登録

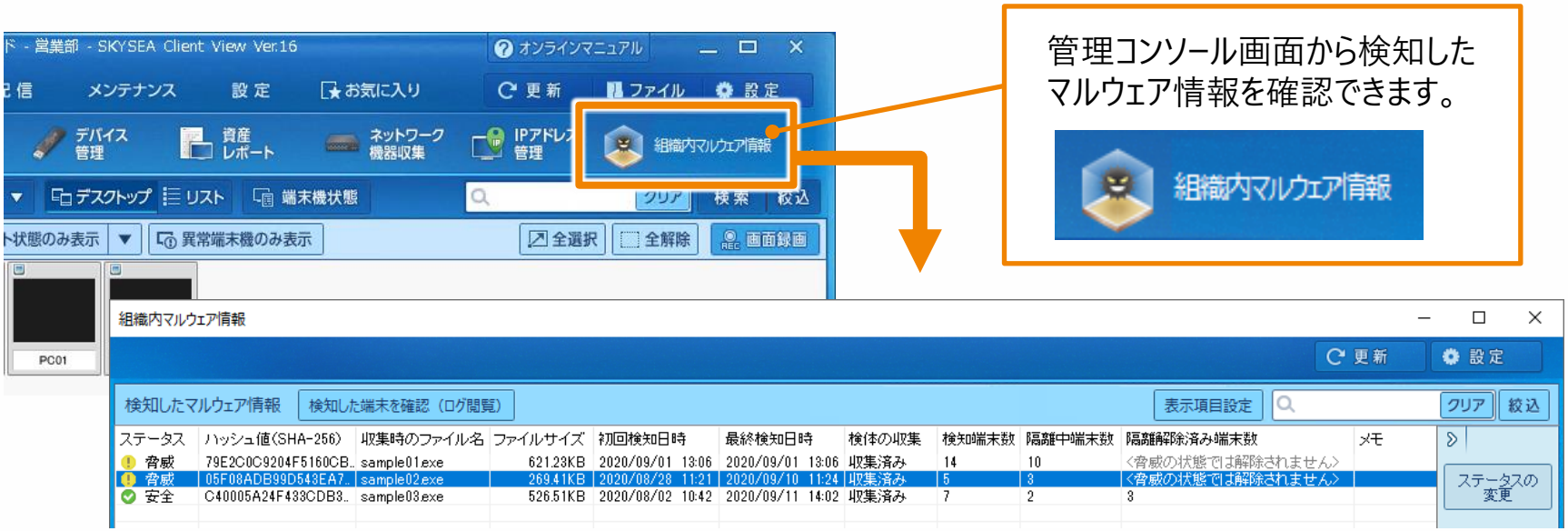
アラートを設定するためのツールは、
Ｓｋｙより提供します。

※保守契約ユーザー用Webサイトより
ダウンロードいただけます。



①検知ファイルの収集・隔離

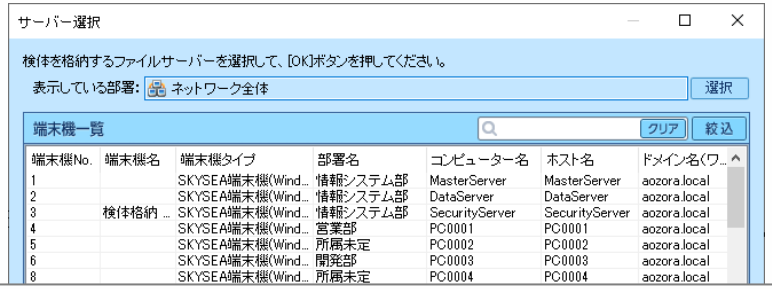
FFRI yaraiによって検知されたマルウェアを、検体としてファイルサーバーに収集。
マルウェアを隔離（ファイルの拡張子を変更して実行を抑止）することができます。



※検知ファイルの収集・隔離機能を使用する前に、初期設定が必要です。

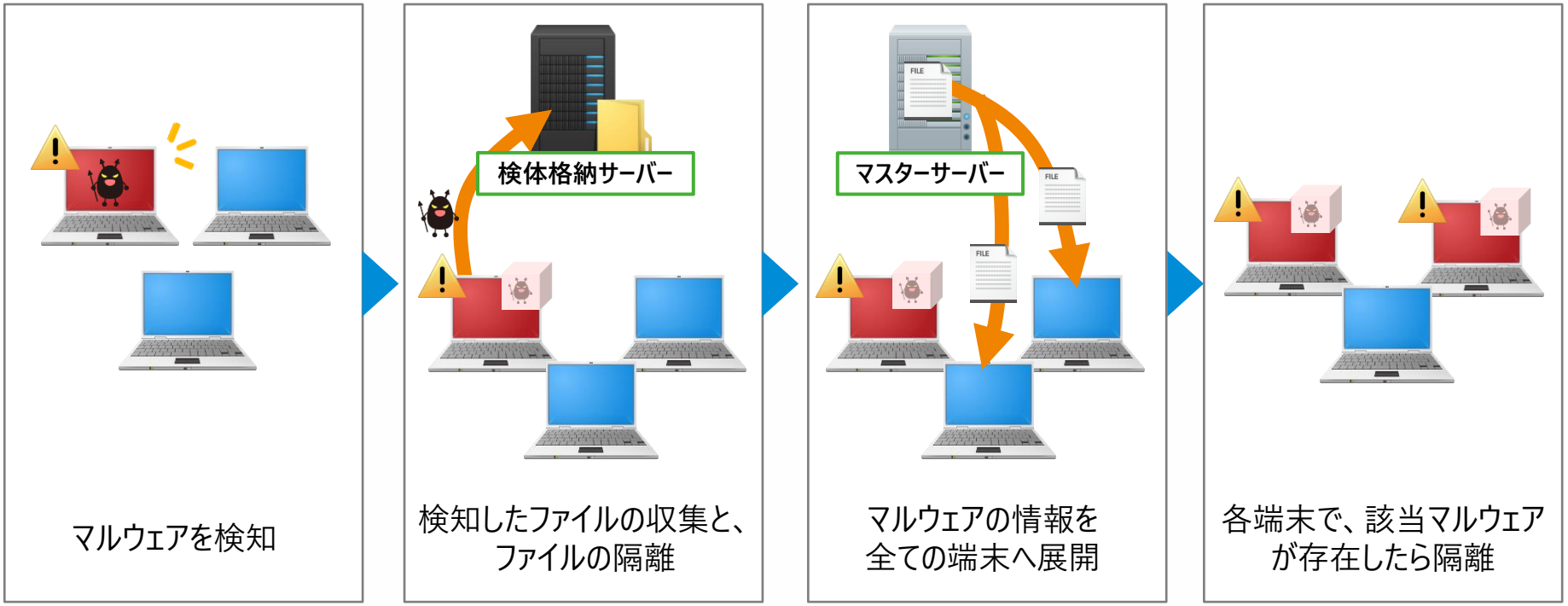
検知されたマルウェアを、
検体としてファイルサーバーに収集できます。

※格納先サーバーとして指定できるのは1台のみです。



②検知ファイルの他端末での存在調査・隔離

組織内の端末でマルウェアが検知された場合は、そのマルウェア情報を全ての端末へ展開。
各端末上で、該当マルウェアが存在した場合は隔離（拡張子の変更）します。
またファイルの隔離（拡張子の変更）を行った記録をログに残します。

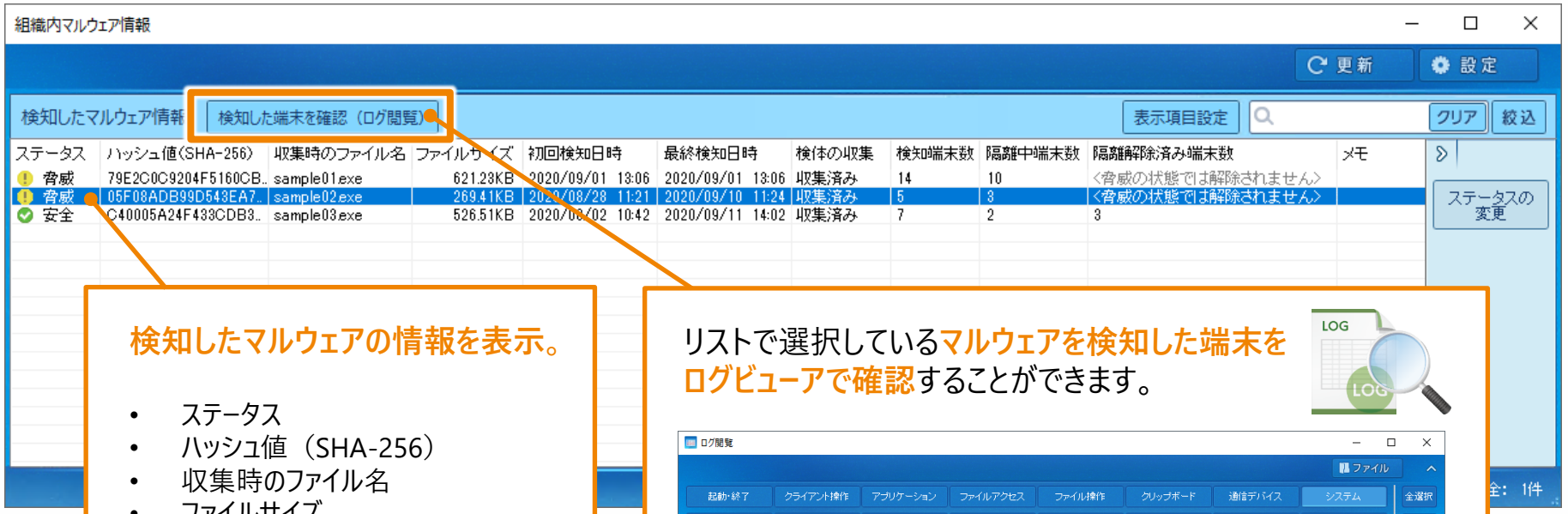


LOG

「マルウェアの検知」、「検知したファイルの収集」、「マルウェアの隔離」が行われた場合は**ログを記録**します。
どの端末でマルウェアを検知したか調査することができます。

②検知ファイルの他端末での存在調査・隔離

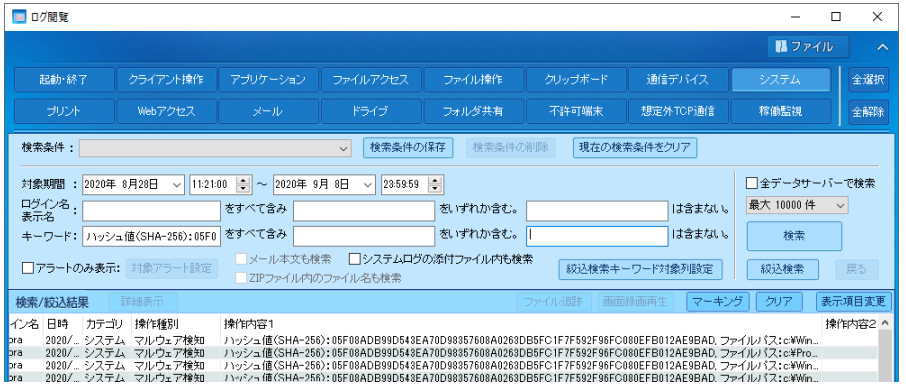
マルウェアを保持している端末を確認することができます。
各端末でいつ検知したのか、隔離が完了しているのかを確認することができます。



検知したマルウェアの情報を表示。

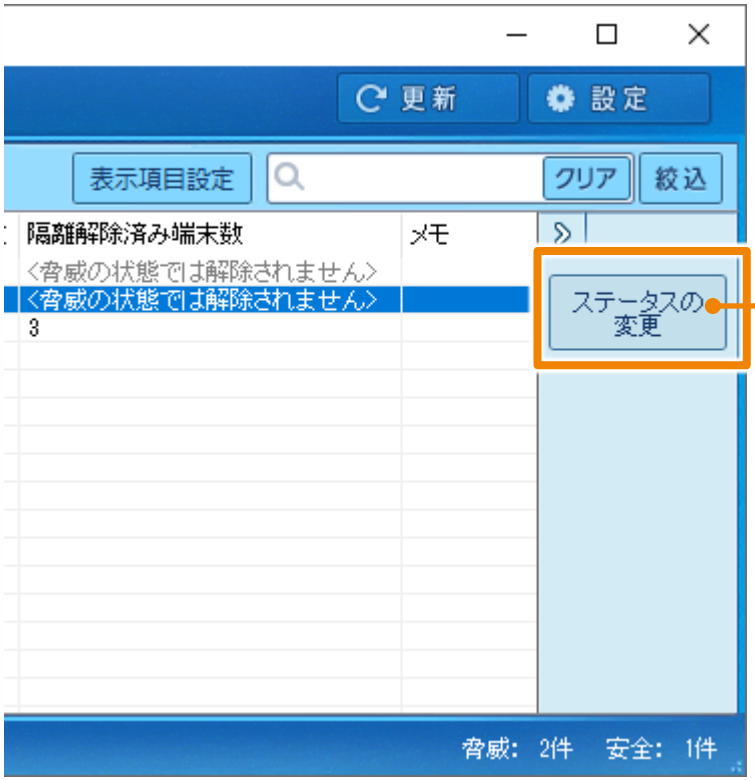
- ステータス
- ハッシュ値（SHA-256）
- 収集時のファイル名
- ファイルサイズ
- 初回検知日時
- 最終検知日時
- 検体の収集
- 検知端末数
- 隔離中端末数
- 隔離解除済み端末数
- メモ

リストで選択している**マルウェアを検知した端末をログビューアで確認**することができます。

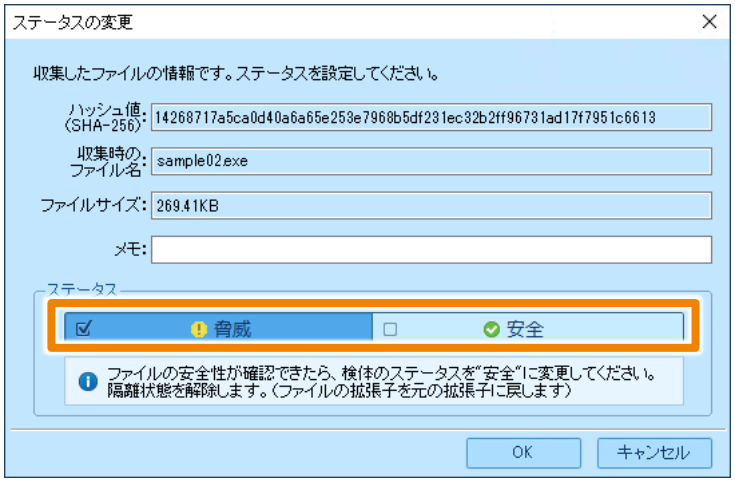


③隔離ファイルの復旧

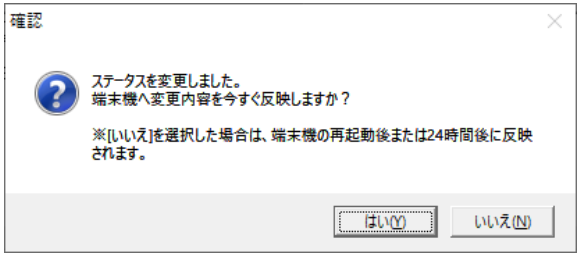
隔離（ファイルの拡張子を変更して実行を抑止）したファイルの安全性が確認された場合は、ステータスを「安全」に変更すると、隔離状態を解除（ファイルの拡張子を元に戻す）ができます。



ステータスを「安全」に変更



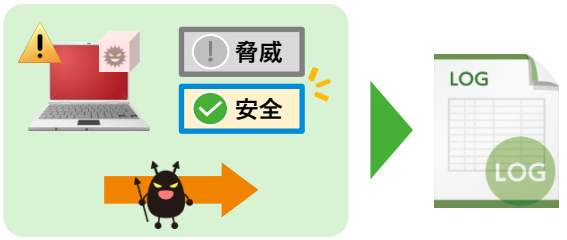
ステータスの変更を今すぐ反映できます。※



※ステータスの変更は1日に1回の定期的なタイミングで端末に反映されます。

④ログの収集

検知したファイルの情報、収集したファイルの情報、復旧したファイルの情報をログで記録します。
ログはSKYSEA Client Viewの管理コンソールから確認できます。



①マルウェアの検知：検知したファイルの情報（ファイルパス / ファイルサイズ / ハッシュ値（SHA-256））を確認できます。

カテゴリ	操作種別	操作内容1	操作内容2
システム	マルウェアを検知	検知したファイル:c:¥TestApp¥sample01.exe, ファイルサイズ:621.23KB	ハッシュ値(SHA-256):05F08ADB99D543EA70D98357608A0263DB5FC...

②検体の収集：収集したファイルの情報（ファイルパス / ファイルサイズ / ハッシュ値（SHA-256））を確認できます。

カテゴリ	操作種別	操作内容1	操作内容2
システム	マルウェアを収集	収集したファイル:c:¥TestApp¥sample01.exe, ファイルサイズ:621.23KB	ハッシュ値(SHA-256):05F08ADB99D543EA70D98357608A0263DB5FC...

③隔離したファイルの復旧：復旧したファイルの情報（復旧後のファイルパス / ハッシュ値（SHA-256））を確認できます。

カテゴリ	操作種別	操作内容1	操作内容2
システム	隔離したファイルの復旧	復旧したファイル:c:¥TestApp¥sample01.exe	ハッシュ値(SHA-256):05F08ADB99D543EA70D98357608A0263DB5FC...

「FFRI yarai」「FFRI AMC」動作環境について

「FFRI yarai」「FFRI AMC」の動作環境

	FFRI yarai		FFRI AMC
OS	Windows 7 Windows 8.1 Windows 10 Windows 11	Windows Server 2012/2012 R2 Windows Server 2016 Windows Server 2019	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
動作環境	■CPU 1GHz以上（デュアルコア必須） ■メモリ 2GB以上 ■ハードディスク 1GB以上の空き容量 ■ファイルシステム システムドライブ,インストールドライブはNTFS必須 ■仮想化環境 動作可能		■CPU 4コア以上 ■メモリ 8GB以上 ■ハードディスク 100GB以上の空き容量 ■NIC GbE ※使用条件 • システム要件に記載した要件は管理コンソールサーバーが動作する最低要件となります。 • AMCで対応できる最大クライアント数は、ネットワーク構成、およびサーバー環境に依存します。 • 上記スペックで3万台が目安となり、管理するクライアント数によってはシステム要件以上のスペックが必要になる場合があります。

※ FFRI AMCはFFRI yaraiの管理コンソールです。
※ FFRI yaraiおよびFFRI AMCのその他使用条件や、詳しい動作環境についてはFFRIセキュリティ社のHPをご確認ください。：https://www.ffri.jp/products/yarai/requirement.htm

同居可能なウイルス対策ソフト（メーカー名）
Microsoft / TrendMicro / Symantec / McAfee / ESET / F-Secure / Sophos

※詳細な製品名、バージョン情報についてはFFRIセキュリティ社のHPをご確認ください：https://www.ffri.jp/products/yarai/requirement.htm

SKYSEA Client View は“企業・団体”のお客様向け商品です

SKYSEA Client View

SKYSEA 検索

https://www.skyseaclientview.net/

商品に関するお問い合わせは、Webサイトよりお受けしております。

- 企業名、本社代表電話番号などをお答えいただけない場合、ご利用いただけません。
- 法人以外の方からのお問い合わせには対応いたしかねます。
- サービス・品質の向上とお問い合わせ内容などの確認のために、通話を録音させていただいております。

東京 03-5860-2622　大阪 06-4807-6382　受付時間9:30～17:30（土・日・祝、ならびに弊社の定める休業日を除く平日）

Sky株式会社 https://www.skygroup.jp/

東京本社　〒108-0075　東京都港区港南二丁目16番1号 品川イーストワンタワー15F　TEL.03-5796-2752　FAX.03-5796-2977

大阪本社　〒532-0003　大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F　TEL.06-4807-6374　FAX.06-4807-6376

札幌支社　仙台支社　横浜支社　三島支社　名古屋支社　神戸支社　広島支社　松山支社　福岡支社　沖縄支社