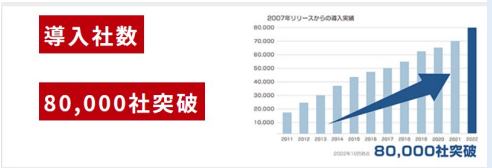
QUALITY SUITE

クオリティソフト株式会社

QualitySoft

クオリティソフト会社概要

会社名	：クオリティソフト株式会社
本社	：和歌山県西牟婁郡白浜町中1701-3
東京本部	：東京都千代田区麹町3-3-4 KDX麹町ビル6F
設立	：1984年2月24日
事業内容	：クラウドネイティブシステムの開発・構築・運用事業 ：クラウドエンドポイントセキュリティ管理サービス事業 ：自治体のLGWANエンドポイント管理サービス事業 ：警察,教育委員会の情報漏えい対策事業 ：統合ドローンソリューション関連事業 ：自然食品EC事業 ：宿泊型ワーケーション クリエイティブ空間事業

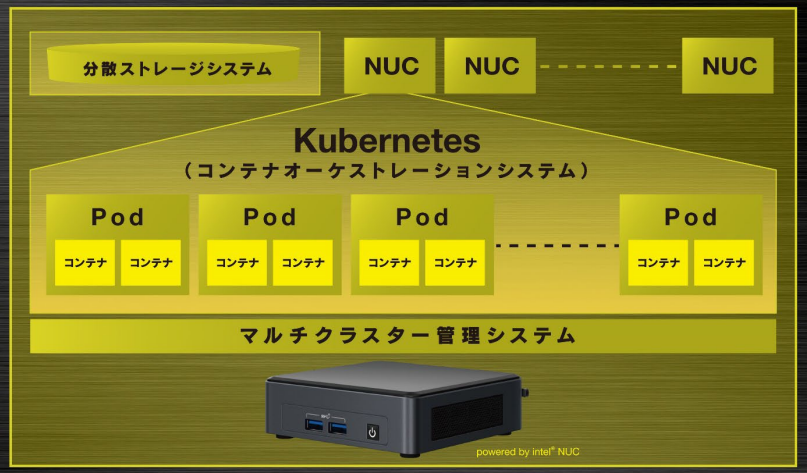


QUALITY SUITE

Quality Cloud System

QCS®

クラウドネイティブ コンテナオーケストレーションを実現するQCS®



1 ハードウェア・ソフトウェアー体型クラウドソリューション

- Intel®NUCを採用し、省スペース・省電力のクラウド基盤を実現
- KubernetesベースのPaaS・IaaSを提供

2 スケーラビリティに優れたクラウドプラットフォーム

- マルチクラスターコンテナーオーケストレーションに特化
- ビジネスニーズに合わせてフレキシブルなリソースの管理・拡張が可能

3 マネージド・レジリエントクラウド

- 完全冗長化されたネットワーク構成
- 自動化されたサービス運用と監視
- マルチサイト・分散ストレージ導入で可用性と安全性を保障

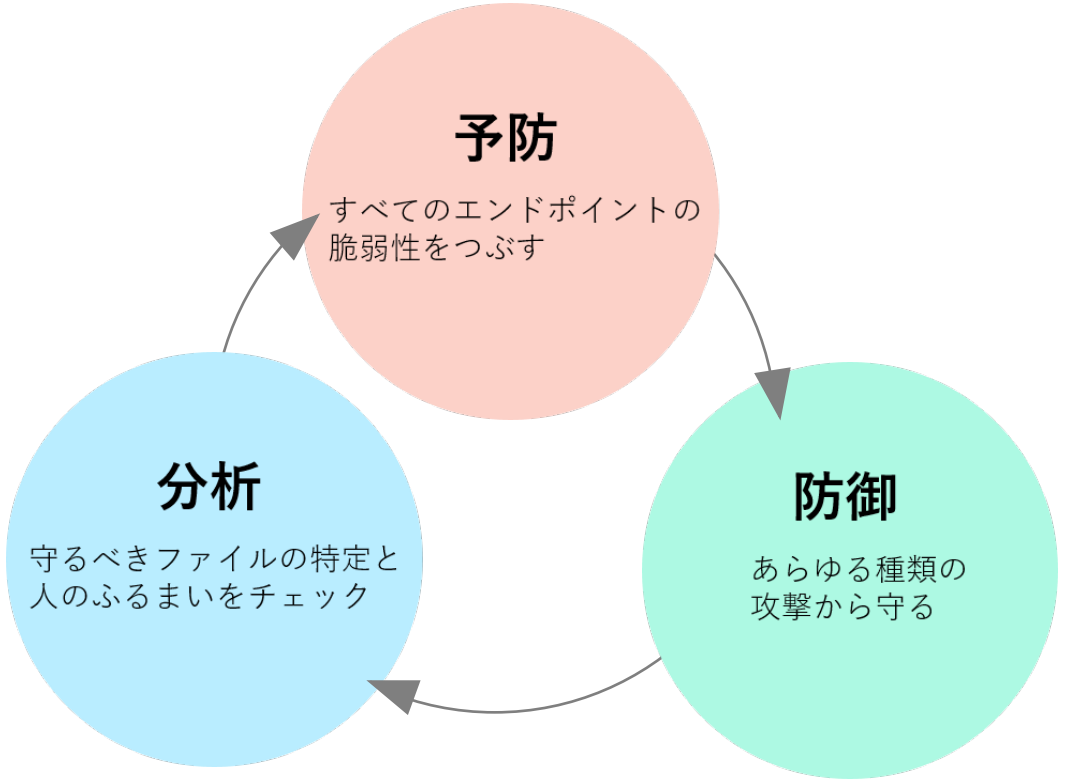
QualitySoft

クオリティソフト クラウド システムから守る

感染させない！拡散させない！
サイバー攻撃に有効な3つの対策

「予防」「防御」「分析」3つのステップでエンドポイントを守る

巧妙化するサイバー攻撃からPCを守るために、弊社では「予防」「防御」「分析」の
3つのステップをまわすことが大切であると考えております。
ここからは、ISM CloudOneを中心としたエンドポイントセキュリティ対策を
ステップごとにご紹介します。



“予防” ～すべてのエンドポイントの脆弱性をつぶす～

まずは予防編です。
攻撃する隙を作らずセキュアな状態を維持する「内部対策」、
Webサイトなどインターネットを経由したウイルスの侵入を防ぐ「入口対策」、
万が一ウイルスが侵入した場合に、感染したPCを踏み台に機密データを格納した
サーバーへの感染拡大を防ぐ「出口対策」、この3つの観点から多層防御することが
有効的ですのでそれぞれご紹介いたします。

01 内部対策

02 入口対策

03 出口対策

内部対策 ～セキュアな状態を維持する ～

Defender Control　自動脆弱性診断

ウイルス対策ソフトがインストールされていないPCが組織内に1台でも存在する場合、この1台が感染してしまうとネットワークを介して他のPCや共有サーバへの感染原因となりかねません。また、インストールしていたとしても入れっぱなしで放置していては意味がありません。**アップデートして最新の状態に保ち、正常稼働をキープする**ことでパターンファイル化されているマルウェアの感染を防ぐことができます。

●すべてのPCをカバーする

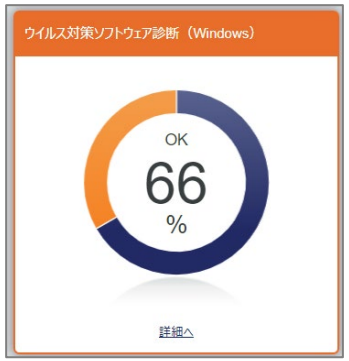
・ウイルス対策ソフトがインストールされていないPCはWindows 10/11に標準搭載されている「Microsoft Defender」を活用
・制御設定が正しく適用されているか確認

ハードウェア名	NG内容（ウイルス対策ソフトウェア診断
WIN10DEMO	未インストール
SANAI-WIN10-01	Windows Defender (x64)

ウイルスと脅威の防止の設定	
ウイルスと脅威の防止の設定	有効
リアルタイム保護	有効
クラウド提供の保護	有効
サンプルの自動送信	安全なサンプルを自動的に送信する
マルウェア対策サービスが通常の優先順位でスタートアップすることを許可する	有効
マルウェア対策サービスの常時実行を許可する	無効
ヘッドレス UI モードを有効にする	有効
コントロールされたフォルダーアクセス	無効

●脆弱性の発見から是正措置までをスムーズに

・「ウイルス対策ソフトに問題あるPC」 を自動であぶり出し
・原因箇所をハイライトで表示



ウイルス対策ソフトウェア情報 1	
製品名	ウイルスバスター クラウド (x64)
プログラムバージョン	16.0
エンジンバージョン	12.000.1008
パターンバージョン	15.877.00
常駐状態	常駐
最新エンジンバージョン	99.999.9999
最新パターンバージョン	99.999.99

入口対策 ～ウイルスの侵入経路を減らす～

URLフィルタリング

ウイルスの感染経路である有害なWebサイトや、外部の不審なサーバとの通信をブロックすることで、**インターネットを経由したウイルスの侵入と感染を防ぐ**ことができます。

●豊富なURLデータベース

国内シェアNo.1を誇る148種 60億5149万コンテンツ（2022年12月26日現在）を基に、柔軟なフィルタリングとセキュアな

時世に即したカテゴリ区分

児童ポルノ	ライブ動画
マルウェア	ストレージサービス
DBD攻撃	Webメール
著作権や商標権の侵害行為	URL転送変換サービス

出典）アルプスシステムインテグレーション株式会社 「マルチデバイス対応Webフィルタリング InterSafe Csts データベース」
https://www.alsi.co.jp/security/iscats/database/

●カテゴリごとにアクセス制御

アクセスレベルを5段階から選ぶことができるため、組織の
運用に併せたアクセス制御が可能

閲覧許可	サイトの閲覧, 書き込み共に可能
規制	規制画面を表示（閲覧不可）
書き込み規制	サイトの閲覧を許可し、 書き込みのみ規制
一時解除 （パスワード入力）	パスワードで例外的に 規制を解除
一時解除 （警告表示）	警告画面を表示 （ボタンクリックで閲覧続行）

出口対策 ～感染拡大による二次被害リスク最小化～

URLフィルタリング

万が一、PCがマルウェアに感染した場合でも、C&Cサーバとの通信を遮断することで
攻撃者による悪意ある情報窃取を防ぐことができます。

●外部の不審なサーバとの通信を制御

攻撃者が遠隔操作しているC&Cサーバへのアクセスを遮断し

クラッキング	ウイルスの製造方法やネットワーク、コンピュータ、モバイル端末への不正侵入や不正使用に関連する情報
マルウェア	ウイルスやスパイウェア感染の恐れがあるサイト。 C&C（コマンド＆コントロール）サーバーなどの不正攻撃サイト。※3
DBD攻撃	閲覧することにより、自動的にマルウェア（不正なプログラム）などをダウンロードさせられる恐れがあるサイト
フィッシング詐欺・ワンクリック詐欺	フィッシングサイトやクリックしただけで料金を請求される詐欺サイト※4
公開プロキシ	フィルタリング機能を回避する公開プロキシ
フィルタリング回避	フィルタリング機能を回避する目的ではないが、結果的にフィルタリング機能を回避してしまうサービス

●インターネット経由の情報漏えいを防止

ストレージサービスを利用した情報の持ち出しや

ストレージサービス	インターネット上のディスクスペース提供など、各種ストレージサービス
SNS・ミニブログ	SNS(会員向けコミュニティサイト)およびミニブログサービス※5
掲示板・チャット	ウェブ上の掲示板およびチャットサービス※5
質問サイト	質問者に回答するコミュニティーサービス
ブログ	ブログサービス※5
ウェブメール	ウェブ上でのメールの送受信サービスおよびグリーティングサービスの提供
メーリングリスト	メーリングリストサービス

出典）アルプスシステムインテグレーション株式会社 「マルチデバイス対応Webフィルタリング InterSafe Csts データベース」
https://www.alsi.co.jp/security/iscats/database/

“防御” ～あらゆる種類の攻撃から守る～

続いて防御編です。
PCは**「機密情報が存在する場所」でもあり「感染した際にマルウェアが実際に活動する場所」でもある**ため、万が一の攻撃に備えて、PC側で “防御” すべきと言えます。
マルウェアは大別すると、パターンファイル化されている「既知の脅威」、
されておらず新種を含む「未知の脅威」の2種類あります。
既知の脅威に対しては、予防編でご紹介した対策でカバーし、未知の脅威に対しては
攻撃者の思考を先読みして防御するふるまい検知機能を利用した対策をご紹介いたします。

既知の脅威対策

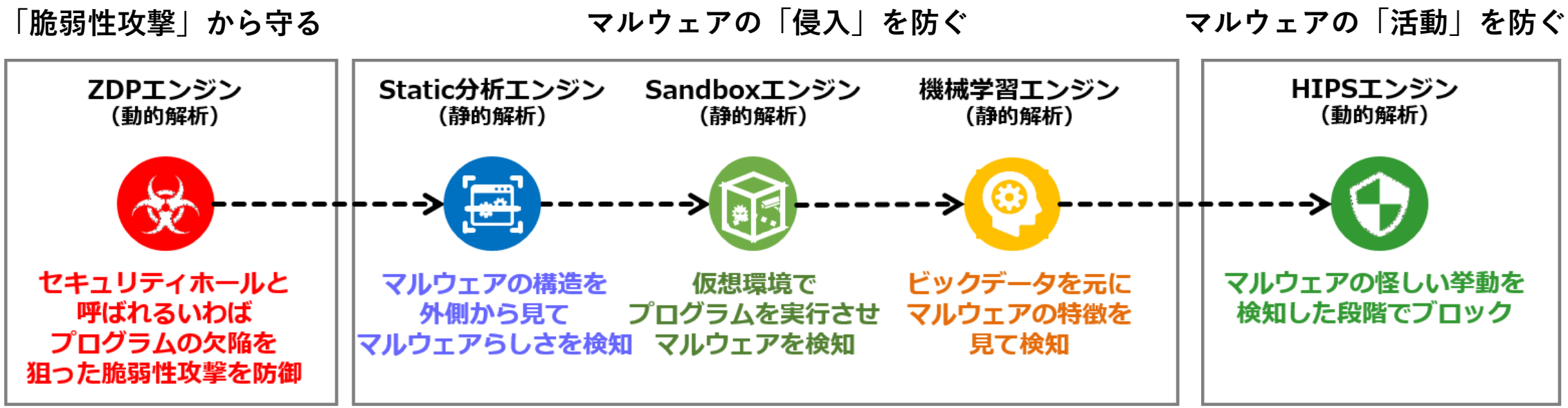
未知の脅威対策

ふるまい検知

未知の脅威対策 ～先読み技術で防御～

攻撃者の思考を先読みして防御するふるまい検知機能を利用することで、一般的なソフトでは対応しきれなかった領域までカバーすることが可能です。

●パターンファイルに依存しない5つのエンジン



出典）株式会社FFRIセキュリティ「次世代エンドポイントセキュリティFFRI yarai マルウェア検出速報」
https://www.ffri.jp/products/yarai/defense_list.htm

ふるまい検知

未知の脅威対策 ～先読み技術で防御～

既にリリースしているバージョンで、数々の未知のマルウェアの脅威を排除した実績があります。従来ソフトでは防ぎきれなかった標的型攻撃やランサムウェアによる攻撃、ゼロデイ攻撃の対策としても有効です。

●パターンファイルに依存しない5つのエンジン

マルウェアの種類	未知脅威および標的型攻撃	発生報道時期	防御エンジンリリース時期
Emotet	2022年6月版	2022/6	**2021/5**
	2022年5月版	2022/5	**2021/5**
	2022年2月版 Downloader	2022/2	**2019/1**
	2021年11月版 Downloader	2021/11	**2019/1**
	2020年12月版	2022/2	**2018/2**
	2019年12月版	2022/1	**2019/1**
ランサムウェア	「RobinHood」 トヨタの工場停止につながったランサムウェア	2022/6	**2019/1**
	「Pandora」	2022/3	**2019/1**
	「Conti」 (2022年2月版)	2022/2	**2019/1**
特定のイベントや事象に関連する攻撃	ワクチン予約を装うフィッシングサイトに関するマルウェア	2021/9	**2021/5**
	東京オリンピックに関係する日本語のファイル名をもつマルウェア	2021/7	**2019/1**
標的型攻撃	国内防衛産業を標的としたマルウェア	2017/8	**2016/10**
	日本年金機構を狙ったマルウェア 「Emdivi」	2015/6	**2014/8**

出典）株式会社FFRIセキュリティ 「次世代エンドポイントセキュリティFFRI yarai マルウェア検出速報」
https://www.ffri.jp/products/yarai/defense_list.htm

・高性能な防御エンジン
・純国産セキュリティ製品
・中央省庁や金融機関等の多数の導入実績

“分析” ～守るべきファイルの特定と人のふるまいをチェック～

最後に分析編です。
PCがマルウェアに感染する時、そこには必ずきっかけとなる操作があります。
メールに添付された悪意のあるプログラムを含んだファイルをダウンロードする、
マルウェアが仕込まれたWebサイトにアクセスするなど、**人のふるまいをきっかけに感染する**と言えます。
万が一感染してしまった場合、どの操作がトリガーとなり感染してしまったのか、
着弾した日時や感染経路、他に感染しているPCがあるかどうか影響範囲を確認し、
再発防止に努めることが大切です。

ふるまい検知　ISM LogAnalytics

マルウェアの実行をすぐ把握

ログ取得ツールを導入することで、ファイル操作やWebアクセスなどのあらゆる種類のログを蓄積できる一方で、膨大な量のログを日々の業務の中で一つ一つ確認できないという課題があります。取得したログから当時何が起きたのか再現できることに加え、**不適切な操作が行われたタイミングで早期に感知し**適切な対処法を見い出せることがログ活用の第一歩です。

●マルウェアが実行されたタイミングで管理者にアラートメールで通知

※ 今後のバージョンアップにより、実際のアラート通知の文面などが変わることがございます。

添付されたURLをクリックして
該当PCの感染状況を確認！

ログ取得日時	コンピューター名	操作ログ種別	操作種別	ファイル名	ファイルハッシュ値	ファイルパス
2022/10/25 18:13:20	LAPTOP-A1UP5N37	ファイル操作	上書き保存	マルウェア.txt	275a021bbfb6489e54d471	C:\Users\q-sen\Desktop
2022/10/25 18:13:20	LAPTOP-A1UP5N37	ファイル操作	新規作成	マルウェア.txt		C:\Users\q-sen\Desktop
2022/10/25 18:13:02	LAPTOP-A1UP5N37	ドキュメントアクセス		マルウェア.txt		
2022/10/25 18:12:48	LAPTOP-A1UP5N37	ウィンドウタイトル	非アクティブ			
2022/10/25 18:12:48	LAPTOP-A1UP5N37	ウィンドウタイトル	アクティブ			

ふるまい検知　ISM LogAnalytics

感染拡散状況を確認

1台でもマルウェアに感染してしまうと、ネットワークを介して他のPCや共有サーバーへ感染する原因となります。感染すると、インターネットを経由して個人情報など守るべき情報を搾取される危険性が高まり、情報漏えいなどの二次被害を招く可能性も高まります。そのため、1台でも感染が発覚した場合は、他に感染したPCがないかどうかを確認する必要があり、即時で拡散状況の確認が可能です。

●二次被害が出る前に危険を察知

マルウェアのハッシュ値	最新の検知日時	検知されたクライアント数	駆除されたクライアント数
6166aee0d9e49545b98e69a68388...	2022/10/25 07:37:35+09:00	1	0
275a021bbfb6489e54d471899f7db...	2022/10/25 09:18:03+09:00	2	1
1751ac12e70e15b4f76c16775cd32...	2022/10/25 07:52:27+09:00	1	0
	2022/10/25 07:55:44+09:00	2	0

感染したPCのマルウェアのハッシュ値を
基に検索をかけて、他に感染しているPCを特定！

検知日時	コンピューター名	ファイルパス	駆除ステータス
2022/10/25 11:48:28+09:00	LAPTOP-A1UP5N37	C:\Users\q-sen\Desktop\...	駆除されていない
2022/10/25 16:47:25+09:00	LAPTOP-5DKU900S	C:\Users\admin\Downloa...	駆除されていない

ふるまい検知 ISM LogAnalytics

きっかけを特定

マルウェアが検知される前後で、誰がどのような操作をしていたのかを確認することで
感染日時やきっかけとなった操作を特定できます。

●人のふるまいを可視化し感染のきっかけを特定

ログ取得日時	コンピューター名	操作ログ種別	操作種別	ファイル名	ファイルハッシュ値	ファイルパス
2022/10/25 18:13:20	LAPTOP-A1UP5N37	ファイル操作	上書き保存	マルウェア.txt	275a021bbfb6489e54d471	C:\Users\q-sen\Desktop
2022/10/25 18:13:20	LAPTOP-A1UP5N37	ファイル操作	新規作成	マルウェア.txt		C:\Users\q-sen\Desktop
2022/10/25 18:13:02	LAPTOP-A1UP5N37	ドキュメントアクセス		マルウェア.txt		
2022/10/25 18:12:48	LAPTOP-A1UP5N37	ウィンドウタイトル	非アクティブ			
2022/10/25 18:12:48	LAPTOP-A1UP5N37	ウィンドウタイトル	アクティブ			
2022/10/25 18:12:47	LAPTOP-A1UP5N37	ウィンドウタイトル	アクティブ			
2022/10/25 18:12:47	LAPTOP-A1UP5N37	ウィンドウタイトル	非アクティブ			
2022/10/25 18:12:09	LAPTOP-A1UP5N37	ファイル操作	上書き保存	log_0010001E00210011000	6fa9d44034e0ee19342fecd	C:\ProgramData\McAfee\...
2022/10/25 18:11:39	LAPTOP-A1UP5N37	ウィンドウタイトル	アクティブ			
2022/10/25 18:11:39	LAPTOP-A1UP5N37	ウィンドウタイトル	非アクティブ			
2022/10/25 18:11:21	LAPTOP-A1UP5N37	ウィンドウタイトル	アクティブ			

時系列に沿って操作を可視化！

ふるまい検知 ISM LogAnalytics

再発防止策への活用

例えばポリシー違反に該当する操作が確認された場合は、根拠に基づいた指導や教育を実施したり、ログを取得していることを周知することで**不適切な行為を抑止する**ことも可能です。再発防止策を検討し実行するためにも、PCの操作ログの活用は欠かせません。

QUALITY SUITE

QualitySoft