Analysis Report

SECURITY REPORT

2023

JUL

DIS(Digital Immune System) サイバーセキュリティの進化のための最高の戦略

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

Column. DIS(Digital Immune System) サイバーセキュリティの進化のための 最高の戦略

01. デジタル免疫システム(Digital Immune System)

2023年ガートナーIT戦略技術トレンドセキュリティ分野で「デジタル免疫システム(Digital Immune System)」が選定された。デジタル免疫システムは人工知能技術が適用されたデータ分析ツールなどでシステム運用を効率化する戦略である。

デジタル免疫システムは多様な脅威、攻撃からコンピューター、ネットワークなど企業の資産を保護するために設計されたソフトウェアまたはシステムの類型である。企業の重要な目標であるビジネスの連続性、顧客価値(データ及びインフラ)を保護するための最高の戦略として注目されている。

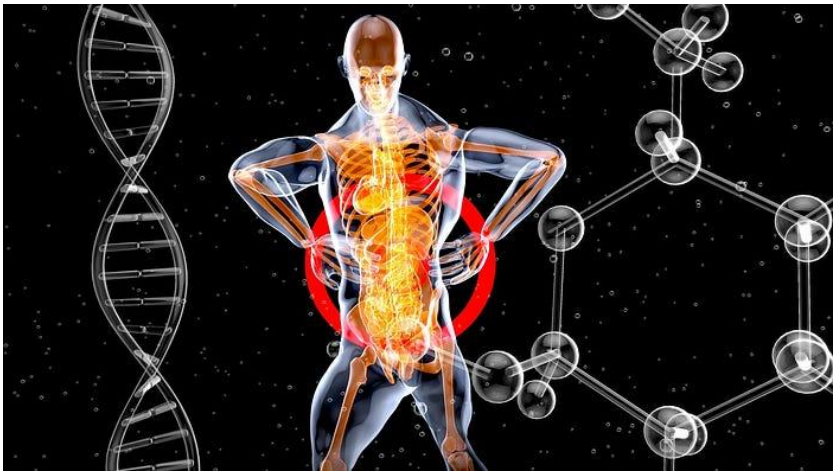
ガートナーは2025年までデジタル免疫システム構築に投資する組織がダウンタイムを80%まで減らして顧客の満足とを高めると展望している。

Top Strategic Technology Trends for 2023	
デジタル免疫システム (Digital Immune System)	• 複数のソフトウェアエンジニアリング戦略を結合して脅威から保護、観察可能性、自動化、極端的な設計及びテストで運用及びセキュリティ脅威を緩和 • デジタル免疫は人工知能技術が適用されたデータ分析ツールなどでシステム運用を効率化して受益を極大化する概念、バリューチェーン全般に渡してセキュリティを適用してより弾力的にシステムを運用し、受益創出の機会を増やす戦略
観察可能性の応用 (Applied Observability)	• システム外部出力値を基に内部ステータスを推論するモニタリング概念、測定指標、追跡、ログの三つの要素を一つに纏めてシステムの動作ステータスをリアルタイムに確認して問題を把握
AI信頼、危険及びセキュリティ管理 (AI TRISM)	• AI Trust, Risk and Security Management : AIモデルガバナンス、信頼性、公定性、信頼性、堅固性、効率性及びデータ保護をサポート
産業クラウドプラットフォーム (Industry Cloud Platforms)	• SaaS、PaaS及びIaaSをカスタマイズ産業ごと機能と結合して組織が産業の続く混乱流れにより簡単に適応できる技術
プラットフォームエンジニアリング (Platform Engineering)	• 開発者とエンドユーザーが簡単にしようできるようにパッケージ化されて選別されたツール、機能及びプロセスセット提供
無線ネットワーク価値の実現 (Wireless-Value Realization)	• 既存のエンドユーザーコンピューティング、エッジ装置サポート、デジタルタギングソリューションなどを含んだ全ての物に無線ネットワークサービス提供
スーパーアプリ (Superapps)	• アプリ、プラットフォーム及び生態系の機能一つのアプリケーションに結合して第3者が自らミニアプリを開発して展開できるプラットフォーム
適応型AI (Adaptive AI)	• リアルタイムフィードバックを使用して配布後モデル動作を変更し、新たなデータと調整された目標を基盤としてランタイム及び開発環境内からモデルを持続的に再教育し、学習して変化する実環境に素早く適応
メタバース (Metaverse)	• 物理的活動を仮想世界に送信したり拡張したり物理的活動を変更、複数の技術テーマと機能で構成された組合革新
持続可能な技術 (Sustainable Technology)	• ITサービスのエネルギー効率性を高めるソリューションのフレームワーク、追跡性、分析、排出管理ソフトウェア及びAIのような技術で企業の持続可能性を可能

【▲ Top Strategic Technology Trends for 2023】

02. ITシステムとサービスの生物学的有機体系接近

生物学的な免疫システムの中心には人間・動物の身体自信を脅威する外部の要因を識別し、除去するために自動作用するシステムで身体細胞を保護しながら感染から身体を防御、回復する期間と細胞及びタンパク質の複雑なネットワーク体系である。



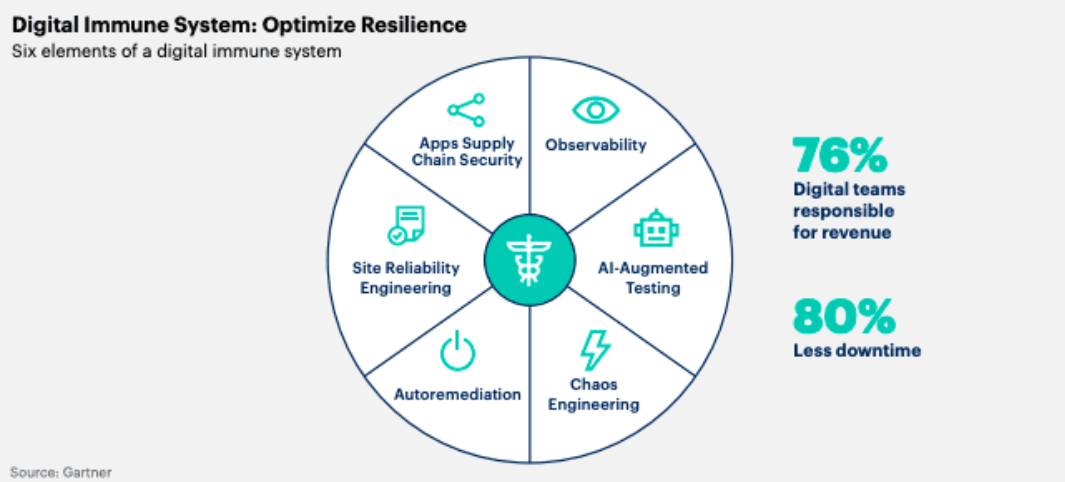
【▲ Immune System (参考 : Julien Tromeur, Pixabay)】

デジタル免疫システムはサイバー脅威を検知して対応するセキュリティシステムで生物学的免疫システムと類似している。ITシステムとサービスに脅威になる攻撃及び兆候に対してネットワーク、システム及びデータを持続的にモニタリング・識別して資産を保護するための自動防御及び対応体系を整えることである。
例えば、フィッシングの試み及びDoS攻撃を含んだ悪意的な活動の兆候を持続的にモニタリングして可視性を確保し、攻撃が検知されたら当該のトラフィックを遮断、感染したコンピューターを隔離、システムを保護するためにセキュリティ担当者に攻撃を警告し、報告、処置ができる技術及びプロセスである。

また、ソフトウェア設計、開発、運用及び分析の多様なプロセスと技術を結合してビジネス成果に影響を及ぼすシステムエラー及び障害を減らす。強力なデジタル免疫システムはエラー及び障害から迅速に回復できるようにアプリケーションの弾力性を高めてソフトウェアバグやセキュリティ問題の影響のような問題から資産を保護する。重要なアプリケーションとサービスが深刻に損傷されたり完全に作動が止まった場合発生するビジネス連続性の危険を減らすことができる。

03. 強力なデジタル免疫システム構築のための6つの実行条件

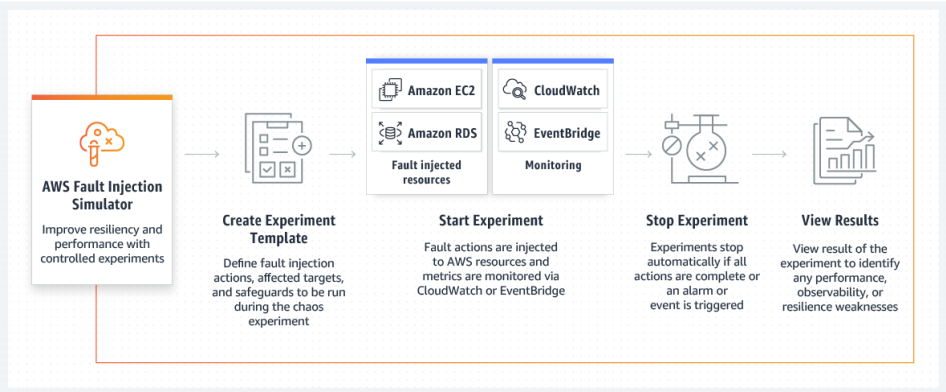
強力なデジタル免疫システム構築は6つのプロセスと技術を結合して製品、サービス及びシステムに発生しうる障害に対する抵抗力を強化し、弾力性を高めて優秀なCX(顧客経験)、UX(ユーザー経験)を作る。



【▲ Gartner Digital Immune System (参考：Gartner)】

観察性(Observability)はソフトウェアのシステムが「見える」ことを実現させる。アプリケーションに観察可能性を構築すると安全性と弾力性問題を緩和し、ユーザー行動を観察してUXを改善することに必要な情報を適用する。これでシステムのステータスをモニタリングして潜在的な問題や脅威が識別できるためデジタル免疫システムのポイントである。これはシステムの性能を測定・追跡してエラーと異常を識別してシステムの全般的なセキュリティと復元力の改善に使用できるデータ収集と分析も含む。

カオスエンジニアリング(Chaos engineering)は実験的なテストを使用して複雑なシステム内から脆弱性と弱点を発見して復元力をテストする。実ユーザー環境に問題が発生する前に潜在的なエラーを発見し、修正してシステムの信頼性と安全性を高める。最近クラウドを基盤としたDevOpsとカオスエンジニアリングが統合されている。



【▲ Chaos Engineering on AWS (参考：AWS)】

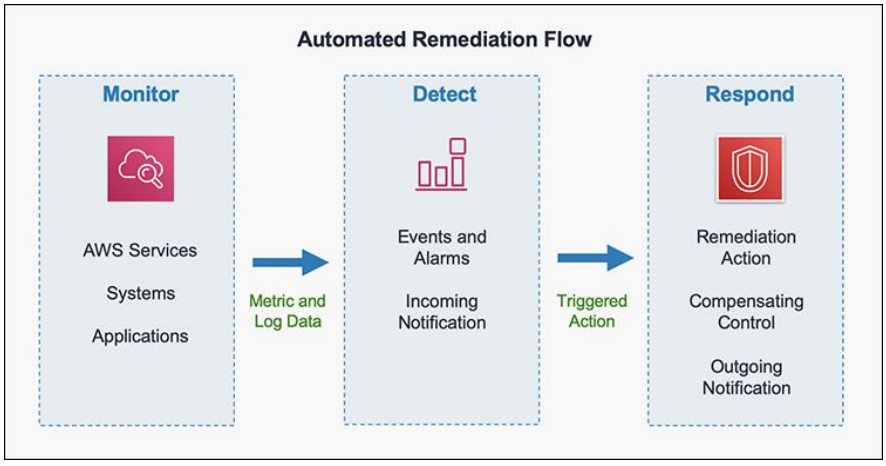
AI拡張テスティング(AI-augmented testing)で組織はソフトウェアテスティング活動を人の介入からどんどん独立的に作ることができる。既存のテスト自動化を補完し、拡張して完全自動化されたテスト計画、生成、メンテナンス及び分析を含む。

Test automation tools, Predictive analytics tools, Test case optimization tools, Test data generation toolsなどで今後発生しうる問題、障害を予測して人工知能基盤のテストケースを生成し、最適のテストプロセスで効率性が改善できる。

【▲ Gartner AI-Augmented Testing Tools (参考：Gartner)】

自動復元・矯正(Autoremediation)は状況に合わせたモニタリング機能と自動化された復元・矯正機能をアプリケーションに直接構築することに重点を置く。自体的にモニタリングして問題を検知すると自動で問題を修正し運用担当者の介入なしで正常な作業状態に戻る。

クラウドから自動復元は幅広く使用されているプロセスでトラフィックが集中されてサービスの遅延もしくは障害が発生した場合、自動拡張(Auto Scaling)してトラフィックを受け入れたりRDS(AWSクラウドデータベースサービス)に問題が発生すると自動復旧することがAutoremediationの例である。

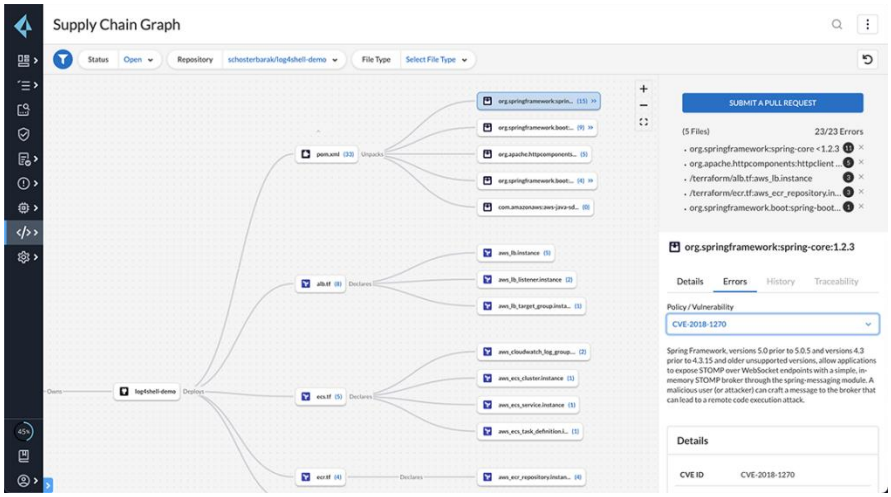


【▲ Security response automation on AWS (参考：AWS)】

サイト信頼性エンジニアリング(Site Reliability Engineering, SRE)はシステムとソフトウェアの安定性に重点を置いたソフトウェアエンジニアリングである。人の介入を最少化して安定性と稼働時間を最大化する方法にシステムを設計し運用することを目標とする。最も重要なのはモニタリング、自動化された問題可決及びインシデント対応システムのようなプロセスとツールの組み合わせである。
クラウド及びオンプレミスからインスタンス、ルーティング、負荷分散、ファイアウォールなどのためのインフラオーケストレーション、適切なサイズのクラウドリソースと必要よって中央処理装置(CPU)、ランダムアクセスメモリ(RAM)のようなリソース追加または除去を含むインフラ最適などがこれに入る。

【▲ Red Hat SRE (参考：Red Hat)】

ソフトウェアサプライチェーンセキュリティ(Application supply chain security)は組織が使用するソフトウェアおよびシステムのセキュリティを保障するために行う処置である。他社のソフトウェア構成、アウトソーシング、社内応用プログラムの開発及びメンテナンスなど全てのものを含む。強力なバージョン制御ポリシー、信頼できるコンテンツに対するアーティファクトレポジトリ使用及び適用寿命周期全般に渡ったサプライチェーン危険管理で内部及び外部コードの整合性を保護する。



【▲ Software Supply Chain Security - Palo Alto Networks (参考：Palo Alto Networks)】

04. サイバーセキュリティでのAI、自動かは未来セキュリティの重要技術

デジタル免疫システムは毎年新たなサイバー脅威と攻撃が発生する環境から多様なサービスの中断、障害から資産が保護できるプロセスとポリシーである。
セキュリティ組織は事業の連続性の観点からサイバー脅威に対応する計画の樹立が必要で、セキュリティは全ての組織と機能、アプリケーション、資産、環境に関連される必要がある。クラウド環境から運用と開発を統合する流れがDevOps、開発・運用・セキュリティが統合される流れがDevSecOpsに発展しているようにデジタル免疫システムは全て組織の主要業務領域を維持するがソフトウェア化されて自動化されたIT環境からシナジーが発揮できる領域に統合されると思う。

特にAI基盤のプラットフォーム及びテスト技術、状況に合った統合されたモニタリング及び自動化は今後セキュリティに必須要件になり、これで問題を自動でモニタリングし、修正して資産を元の状態に戻せられる体系を整えることができる。

05. 参考資料

1. [Gartner] Top Strategic Technology Trends for 2023
2. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter
3. https://www.cdotrends.com/story/17584/what-digital-immune-system-and-why-does-it-matter
4. https://medium.com/enrique-dans/its-time-we-let-ai-create-a-digital-immune-system-for-companies-49382c11bf97
5. https://www.betterhealth.vic.gov.au/health/conditionsandtreatments/immune-system
6. https://aws.amazon.com/ko/blogs/security/how-get-started-security-response-automation-aws/
7. https://www.redhat.com/ko/topics/cloud-computing/sre
8. https://catalog.us-east-1.prod.workshops.aws/workshops/5fc0039f-9f15-47f8-aff0-09dc7b1779ee/en-US
9. https://www.paloaltonetworks.com/prisma/cloud/software-supply-chain-security
10. https://www.boannews.com/media/view.asp?idx=118127