

5.3 セキュリティソリューション Security Solutions

三菱電機での製品セキュリティへの取組み

Initiatives for Product Security by Mitsubishi Electric Corporation

三菱電機デジタルイノベーション(株)情報管理・セキュリティソリューション統括室は、三菱電機グループの情報セキュリティの管理を担っている(図1)。製品セキュリティでは社外窓口及びライフサイクル全般にわたる施策の展開を行うことでセキュリティの品質向上に努めている。施策には、出荷前、出荷後、活動基盤整備の三つの領域がある。出荷前では、脆弱(ぜいじゃく)性の混入予防や

流出防止のためのガイドや開発環境をセキュアにする仕組み、脆弱性診断サービスなどを、出荷後では、製品の構成部品目を基に脆弱性情報を収集するシステムや発見された脆弱性への対応を、活動基盤整備では、教育プログラムの整備による人材育成や規程整備・法令対応による体制整備を行っている(図2)。

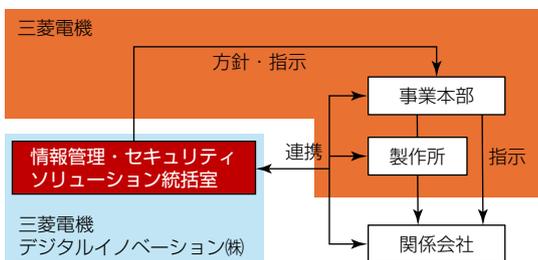


図1-三菱電機グループの情報セキュリティの管理体制

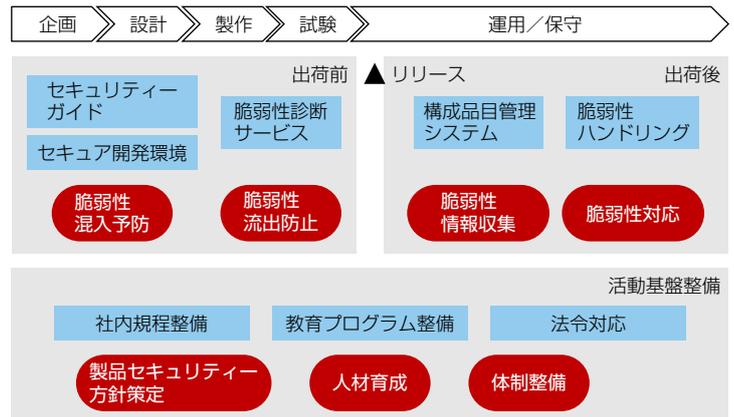


図2-製品セキュリティの取組みの全体像

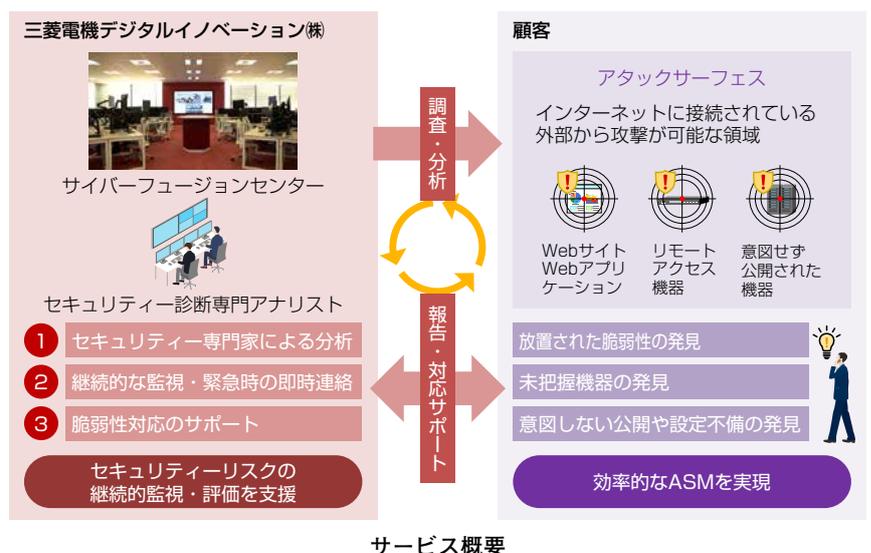
<取り扱い：三菱電機デジタルイノベーション(株) MEDigital_gibo_contact@rb.MitsubishiElectric.co.jp>

ASMサービス

Attack Surface Management Services

インターネットに公開された機器は常に外部からの攻撃の脅威に晒(さら)されており、未把握の機器はセキュリティ対策が行き届いておらず攻撃の起点になりやすい。攻撃を防ぐにはIT資産の存在を正しく把握することが重要である。

三菱電機デジタルイノベーション(株)が提供するASM(Attack Surface Management)サービスは、外部から直接アクセス可能なIT資産を発見し、セキュリティリスクを継続的に調査・報告する。これによって外部からの攻撃を受けるリスクが高いIT資産の把握が可能になる。また、継続的な対応によって新たに設置される機器・システムについても検出可能になる。平時から能動的なセキュリティ対策を行い攻撃の芽を摘むことが、自組織のセキュリティリスクを低減させる有用な手段になる。



サービス概要

<取り扱い：三菱電機デジタルイノベーション(株) TEL：03-6771-6035>

Smart CFC/SOC：拡張性あるセキュリティー運用を自動化する監視基盤の実現

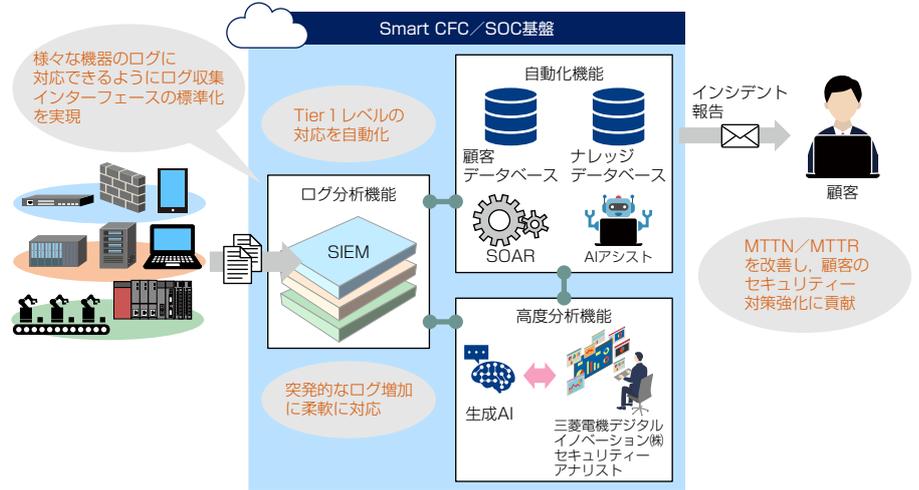
Smart CFC/SOC: Realization of Scalable and Automated Security Operations Monitoring Platform

近年、生成AIの発展によって攻撃手法が効率化、高度化されて、攻撃件数は急激に増加しており、人手を介した対応は限界を迎えている。また、攻撃に対応するためのセキュリティー機器も多種・多様化しており、多様なアラートを統合的に監視できる基盤の整備が急務になっている。

この課題を解決するため、三菱電機デジタルイノベーション(株)は、アラート調査、分析、通知の仕組みを自動化し、迅速かつ安定したセキュリティー運用を提供できて、多様化するセキュリティー機器を包括的・標準的に取り扱う“Smart CFC/SOC基盤”を開発した。

Smart CFC/SOCは、最新の自動化技術を活用し、分析に必要な情報の自動収集、顧客への自動初報通知、アラートの初動対応の自動化を実現した。これによって、顧客へのアラート通知/解決時間を60%短縮することを目指す。また、様々なアラートを取り込めるようにアラート収集インターフェースの標準化を実現し、顧客の多様なニーズに対応する。今後の展望として生成AIを活用した

高度な分析の実現、AIエージェントを活用したセキュリティー運用の自律化を計画する。三菱電機デジタルイノベーション(株)はこの基盤を通じて、高品質、高性能でありながら中堅/中小企業でも利用が可能な、他社にはないセキュリティーサービスを提供し、顧客のセキュリティー対策強化に貢献する。



SIEM : Security Information and Event Management. セキュリティー情報及び各種機器のログを包括的に管理・分析するシステム
 SOAR : Security Orchestration, Automation and Response. セキュリティー運用の効率化を進めるためのツール
 MTTN : Mean Time to Notify. 平均通知所要時間
 MTTR : Mean Time To Resolve. 平均解決所要時間

Smart CFC/SOCのサービス提供体系

<取り扱い：三菱電機デジタルイノベーション(株) TEL：03-6771-6030>

金融機関向けマネージドDNSサービスでのDNSSECへの対応

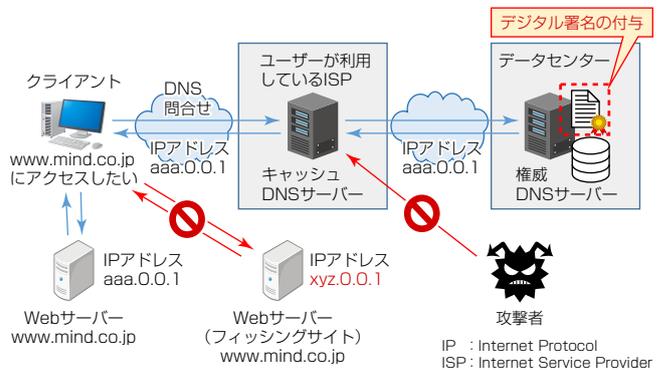
Implementation of DNSSEC in Managed DNS Services for Financial Institutions

近年、企業へのサイバー攻撃の手法は多様化しており、DNS(Domain Name System)の脆弱性や機能を悪用した攻撃も増えてきている。DNSはインターネット上の通信には必須の技術であり、各企業のドメインを管理するDNSは常に安定して正当な応答を返すことを要求されるが、利便性の観点から通信の検証・暗号化が実施されることは少なく、乗っ取りや改ざんのリスクに晒(さら)されている。そういったDNSの信頼性を向上する技術としてDNSSEC(DNS Security Extensions)が注目されており、政府からの呼びかけによって金融機関やドメイン事業者を中心にその導入が推進されている。DNSSECとは、DNSの応答に電子署名を付与することで、そのデータの完全性を保証するセキュリティー技術である。

三菱電機デジタルイノベーション(株)では、一部金融機関のドメインを管理するDNS基盤を提供しており、顧客からの要望に応えるため基盤刷新及び機能増強を行い、顧客ドメインのDNSSECへの対応を実現した。金融機関に求められるセキュリティー基準や署名アルゴリズムの危殆

(きたい)化にも対応するため、電子署名の付与に使用する署名鍵の定期更新、署名が有効な状態になっているかの監視といった運用を同基盤のサービスとして提供している。

今後の展望としては一般企業向けの汎用DNS基盤及びDNSセキュリティーサービスの拡充を計画し、サービスを通じた顧客DNSのセキュリティー対策強化を実現する。



DNSSEC導入後のDNS動作イメージ

<取り扱い：三菱電機デジタルイノベーション(株) TEL：03-6771-6028>

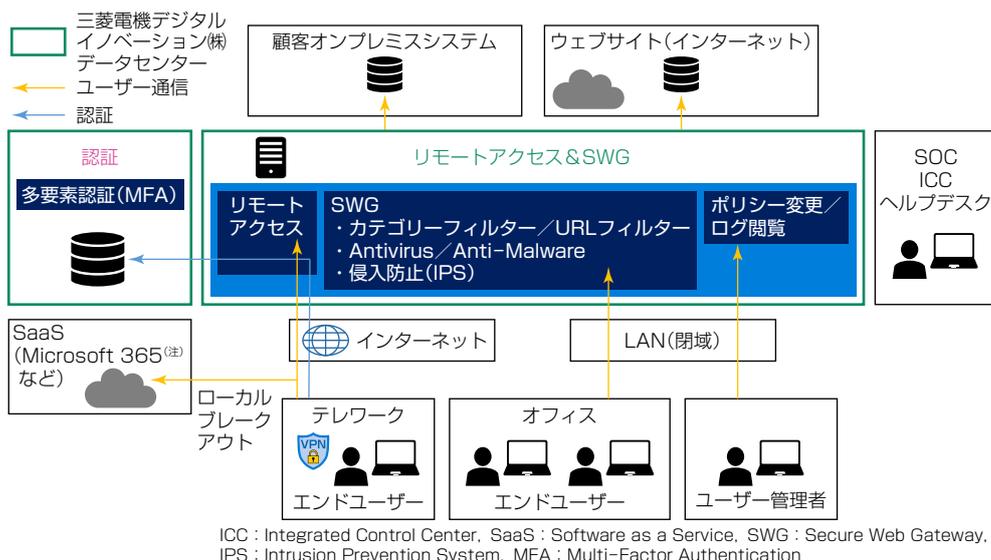
セキュアアクセスサービス Security Service Edge

Secure Access Services: Security Service Edge

昨今、リモートアクセス環境での不正侵入が増加している。三菱電機デジタルイノベーション(株)の従来のリモートアクセスサービスは、なりすまし対策と適切な運用によってリスクは限定的であるものの、利用者の端末マルウェア感染の対策は困難であった。

一方、この脅威に有効とされるSASE(Secure Access Service Edge)／SSE(Security Service Edge)は高性能であるが、設計・運用が複雑かつ費用負担も大きい。そのため、機能を十分に活用できない企業では費用対効果が低下する。そこで、この課題解決に向けて従来のリモートアクセスサービスに対して費用対効果の高いセキュリティー機能を厳選して追加した。具体的には、マルウェア感染に有効な機能(Webフィルター／AV(Antivirus)／IPS(Intrusion Prevention System))を実装し、設計・運用を簡素化した。さらに、三菱電機デジタルイノベーション(株)の国内DC(Data Center)のIaaS(Infrastructure as a Service)上に仮想アプライア

ンスとして構築することで柔軟なスケーリングに対応し、専用回線を通じて低遅延・高可用性を確保する。故障対応等の運用は三菱電機デジタルイノベーション(株)が365日24時間に対応する。脅威検知時は要約メールで顧客管理者に即時通知し、顧客専用管理画面によって詳細アラート・ログ内容参照・Webフィルター等の変更も操作可能にする。希望に応じてヘルプデスク／SOC(Security Operation Center)への一括移管も可能である。



サービス概要

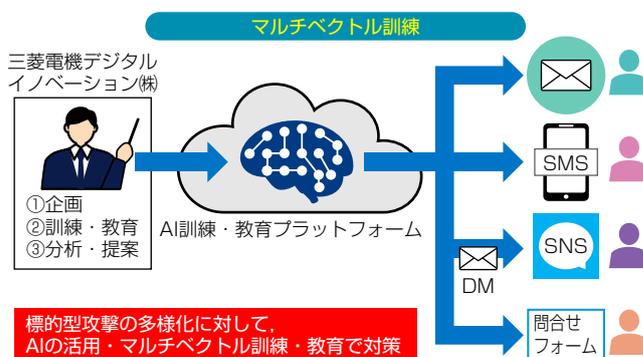
<取り扱い: 三菱電機デジタルイノベーション(株) TEL: 03-6771-5155>

マルチベクトルに対応した標的型攻撃対策訓練・教育サービス

Security Awareness Service for Multi-vector

企業経営に甚大な損害を与える不審メール攻撃を発端としたサイバー攻撃への対策として、三菱電機デジタルイノベーション(株)は“標的型攻撃対策訓練・教育サービス”の提供を2024年9月に開始した。イスラエル発の最先端のAIを用いて実際の攻撃を模した訓練メールを訓練対象ユーザーに配信することでリアルな攻撃を体験させる。昨今、企業によるSNS(Social Networking Service)の利用が増えてきたことに伴って、メール以外のSMS(Short Message Service)やSNSのDM(Direct Message)、問合せフォームを利用した標的型攻撃が増えてきた。これらの攻撃は従来のメールとはプラットフォームが異なることで、企業側で一括検査ができず、アカウントの乗っ取りやブランド・顧客信頼の棄損などのリスクを抱えている。攻撃方法が多様になってきたこともあり、このサービスをマルチベクトル(SMS, SNS, 問合せフォーム)に対応させた。これによって、電話番号やDM宛てにも訓練内容を送付できるようになる。最初は利用頻度の高いSMSについ

て、2025年10月からサービスを開始した。マルチベクトルに対応したこのサービスを活用することで、メール以外の攻撃手法にも対処できるようになる。教育コンテンツを活用した社内教育や評価分析結果も提供するため、顧客自身で行うと多大になる運用負荷を削減できる。



サービス概要

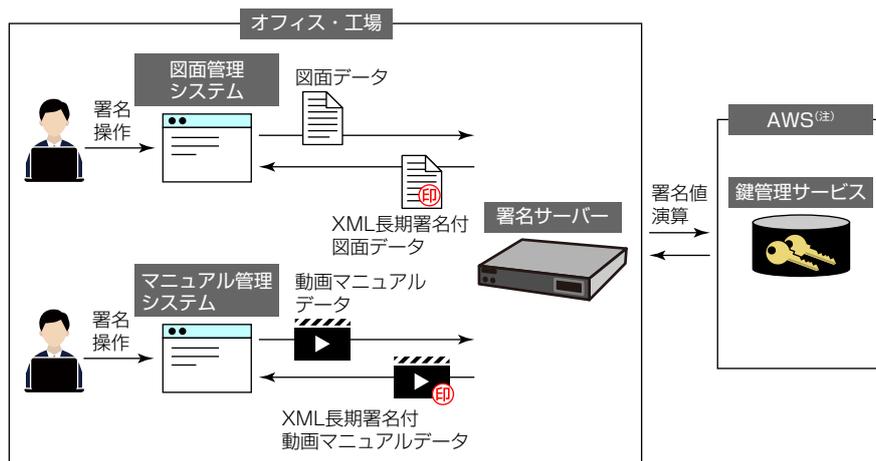
<取り扱い: 三菱電機デジタルイノベーション(株) TEL: 03-6771-6035>

多様な電子ファイルをトラストできるXML長期署名ソリューション

XML Based Advanced Electronic Signature Solution for Full Varieties Files

機密文書の真正性確認や存在署名の必要性に応じてきた電子署名のニーズは、近年では3D図面や動画にまで広がりを見せている。今回開発したサービスでは、WebAPI (Application Programming Interface) による連携機能、高速ハッシュ演算機能、XML(Extensible Markup Language)長期署名機能(以下“XAdES”という。)を用いる。これによって、取り扱うファイルサイズに理論上制限

はなく、署名対象ファイルをクラウドに置かないことで情報漏洩(ろうえい)リスクを極小化し、ファイル形式はそのまま電子署名が可能になる。2025年12月に3D図面向けとして初版をリリースした。次版では動画マニュアル、機器プロファイル情報などへの対応を計画中である。以前からあるXAdESの特長に加えて、機能拡張と使い勝手の向上を実現していく。



多様な電子ファイルをトラストできるXML長期署名ソリューション構成イメージ

<取り扱い：三菱電機デジタルイノベーション(株) TEL：0467-95-4660>