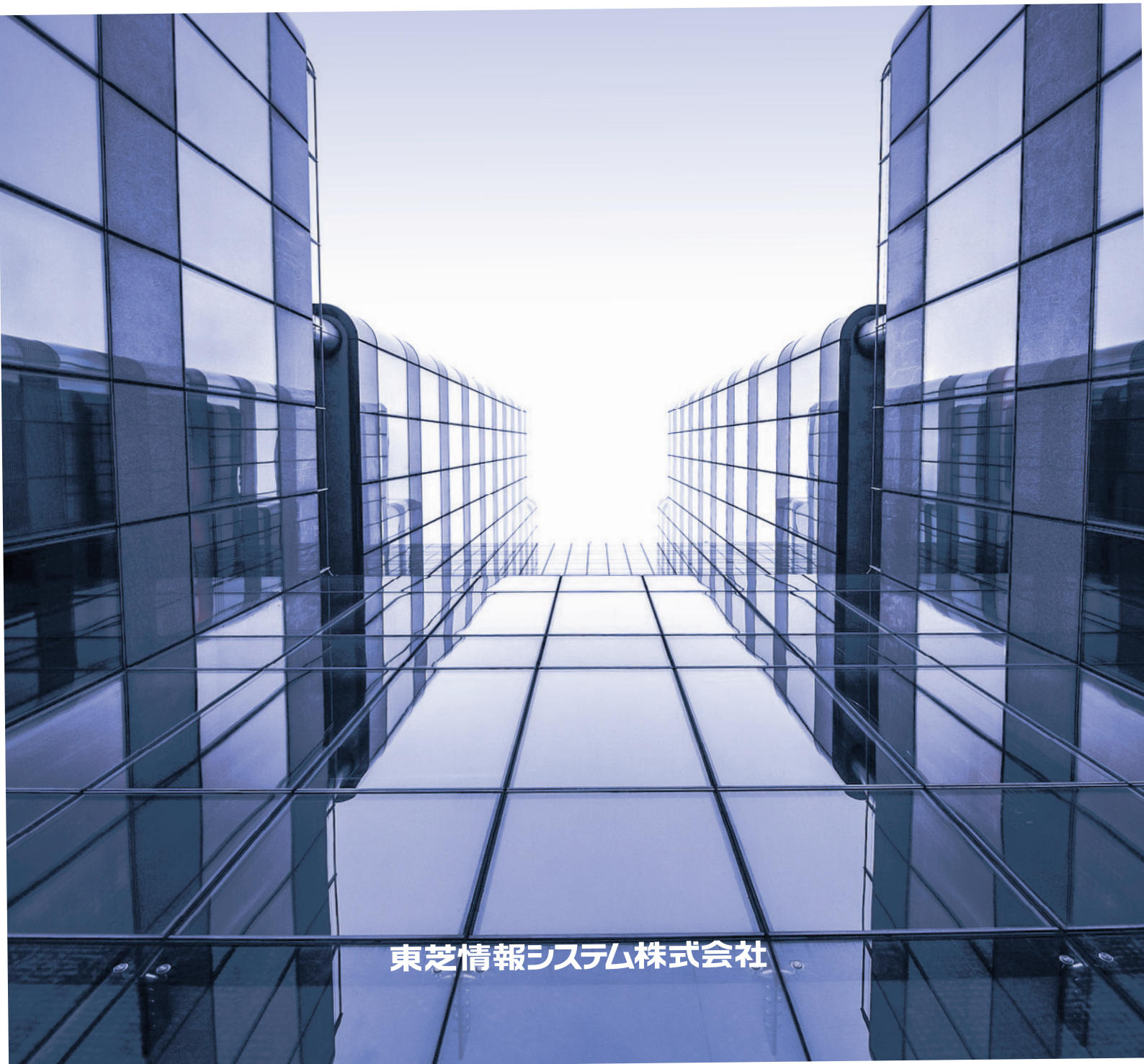
TOSHIBA
Leading Innovation

Wave

技術誌
2018.5
Vol.23

[特集] セキュリティソリューション



東芝情報システム株式会社

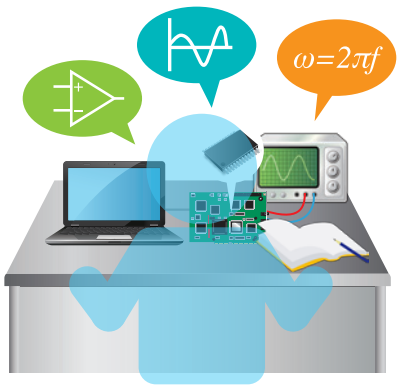
TOSHIBA
Leading Innovation

専用 IC とテキストによる回路設計トレーニング

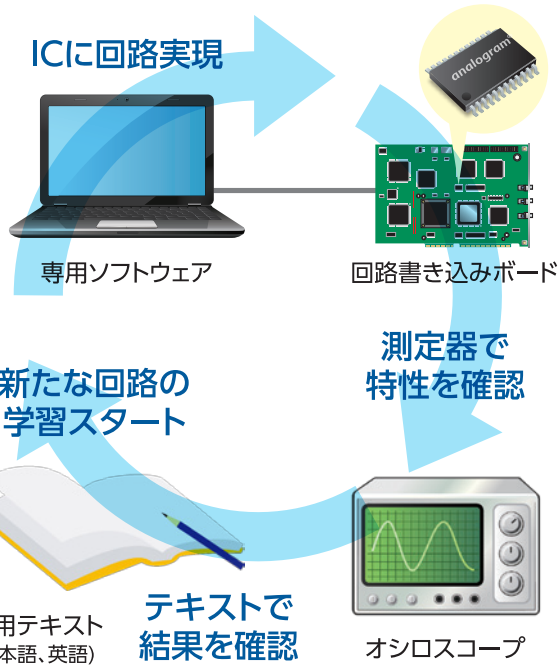
analogram® トレーニングキット

analogram トレーニングキットは、analogram（専用 IC）を使って、様々なアナログ回路を学習できるトレーニングキットです。付属のテキストを参照しながら、何度でも IC 上に回路を再構成することができ、特性を確認しながら学習を進めることが可能です。また、本キットはハンダ付けを必要としないので、効率的に多くの回路を学ぶことができます。

学習環境



学習イメージ



point 1

何度でも回路の書き換えが可能

IC への回路書き込みは無制限で、多くの回路を IC 上に実現

point 2

IC を用いたアナログ回路学習が可能

実際の IC とシミュレーションとの特性の違いを、すぐに確認

point 3

ハンダ付けが必要なし

IC 上に回路を構成するので、ユニバーサル基板への部品実装等は不要

東芝情報システム株式会社

LSI ソリューション事業部
〒210-8540 川崎市川崎区日進町 1 番地 53（興和川崎東口ビル）
TEL: 044-200-5300（ダイヤルイン）
E-mail: tjlsi-sales@tjsys.co.jp https://www.tjsys.co.jp/

社内で磨いた技術をいち早く提供し お客様からの期待に“プラス1”で応えます

常務取締役
技術マーケティング部 部長
長田 茂
Shigeru Osada

創立以来、エンジニアリング一筋にビジネスを展開してきた当社は、LSIからエンベデッド、SI、ヘルスケアまでの事業を一つの企業として有しています。モノづくりには貪欲でコツコツと技術を築き上げるDNAを備えていると自負しながらも、ワンストップでお客様の課題を解決できる真のソリューションをもっとスピーディに提供できなければ、今の世の中の変化に対応できないと、以前から感じていました。

大切なのは、東芝グループや海外企業から優れたものを積極的に取り入れて検討し、自ら活用しながら、当社らしい価値を付加して商品化していくことと、そのスピード感です。お客様の課題やニーズを敏感に感じ取りながらビジネスを進めていけるよう、社内でも技術マーケティング部門を設けて国内外の技術発掘に努めたり、各事業部に商品企画部を置いて商品やサービスに対しての意識を高めたりといった取り組みを進めてきました。

最近のトレンドとなっているRPA(ロボティック・プロセス・オートメーション)を実際に自社の業務に適用して効率化を図り、大きな成果が生まれつつあります。こうした成果をさらに磨いてサービスとして提供することでお客様のビジネス拡大に寄与していこうという風土が醸成できてきたのが、ここ数年の当社の大きな変化だと感じています。

スモールスタートでも小回りを利かせながら、お客様の立場に立った提案ができ、徹底的に寄り添っていけるのが当社らしさだと思います。お客様の期待に“プラス1”で応えていきながらお客様と一緒に成長を目指します。

技術誌
2018.5
Vol.23

Wave

特集　セキュリティソリューション

機密情報ファイルを自動で暗号化するソリューション、組込み機器のソフトウェアを保護するツール、IoTセキュリティ市場の新たな製品提供の取り組みなど、当社の多岐にわたるセキュリティソリューションを紹介します。

Contents

20年培った技術と経験をもとに 新商材発掘・提供でさらなる成長を

当社はこれまで20年近く、数多くのセキュリティソリューションをお客様に提供してきました。その代表格である改ざん検知ソリューション「Tripwire Enterprise」や、「ManagementCore」、「dynaCloud iSM」をはじめとするIT資産管理・セキュリティ統合管理製品の販売は、当社のセキュリティビジネスを支える大きな柱となっています。また、各製品とも大規模ユーザーへの導入が多くを占めている点が当社の特徴です。

当社が優れた製品を厳選して提供してきたこともありますが、お客様が安心して、製品選定から設計・構築・運用・保守まで一貫して任せられる、という点に高い評価をいただいています。市場が成熟しセキュリティ製品が多くのお客様に受け入れられるようになった今、長年培った技術やノウハウが開花して総合力で競合他社を凌ぐまでになったと考えています。

本号では、お客様のニーズに応えた幅広いセキュリティ製品や技術を紹介するとともに、OT(Operational Technology/制御技術)分野での取り組みも紹介しています。ビルやエレベータなど設備・機械の制御、入退室管理やカメラによる監視などへのセキュリティ対策は、極めて不十分と言わざるを得ません。サイバーテロによる深刻な被害は世界的にも後を絶たず、日本でも対策が急務となっています。当社は、米国視察で関連製品や市場調査を実施し、今後活発化するであろうOT分野向けセキュリティの研究開発を進めています。LSIから組込み、クラウド、アプリケーションまでの事業が一体となって研究開発を進め、融合・連携ビジネスを展開することで他社には真似のできない、当社の強みを発揮できると考えています。

海外からの新たな技術や製品の発掘も積極的に行っており、海外企業との橋渡しをする現地のコンサルタントも活用しています。契約交渉などの円滑化はもとより、継続的かつ効率的に情報収集を行いながら新しい優れた商材を今後も取り揃えていきたいと考えています。セキュリティビジネスにおいて、これまでの当社の豊富な経験を活かして、さらなる成長を目指し取り組んでいるところです。そのために、海外などでお客様に合った商材を見つけ、市場に展開することで、当社のセキュリティビジネスの柱を増やしていきます。

ＳＩソリューション事業部
ＳＩソリューション第五部　部長　石川 宏

IoT領域におけるセキュリティ対策で高度化するサイバー攻撃の脅威に対応

当社はセキュリティ製品やソリューションを提供してきましたが、昨今のサイバー攻撃における脅威はこれまでのIT(情報技術)領域だけに留まらず社会インフラや製造設備にも及んでいます。こうしたOT(制御技術)領域でのセキュリティ意識やニーズの高まりを受け、当社でもIoTセキュリティ市場の新たな製品を提供できるよう取り組んでいます。

IoT機器・インフラシステムを取り巻く脅威

標的型攻撃やランサムウェアの急増により、社会インフラや製造設備などのIoT領域に対するセキュリティ対策のニーズがこれまで以上に高まってきています。従来はPCをはじめとするIT機器がネットワークに接続していましたが、今ではIT機器に限らず、車載や家電のほか、製造設備や社会インフラといった多種多様な機器がネットワークに接続する時代を迎えています。

調査会社のIDC Japanによると、2016年の国内IoTセキュリティ製品市場規模は、前年比27.5%増の518億円で、2021年には1,250億円まで成長すると見込まれています**(図-1)**。これは、ネットワークへの接続によりIoT領域へのサイバー攻撃が現実的な脅威として迫っており、IoTセキュリティ市場への需要が高まっていることを示しています。

既に海外では電力の発送電設備や空港・地下鉄の制御システムに対してサイバーテロがあり、停電やシステム停止の事故が発生しています。こうした海外のサイバーテロは、重要なデータを暗号化し使用できなくさせて、復旧に対しては身代金を請求するランサムウェアが主体です。攻撃の手口が巧妙かつ悪質であり極めて深刻な状況です。このようなことから、国内においても電気やガスなどを含めた重要な社会インフラシステム、製造工場やプラントなどへのセキュリティの重要性は急速に高まっていると言えるでしょう。

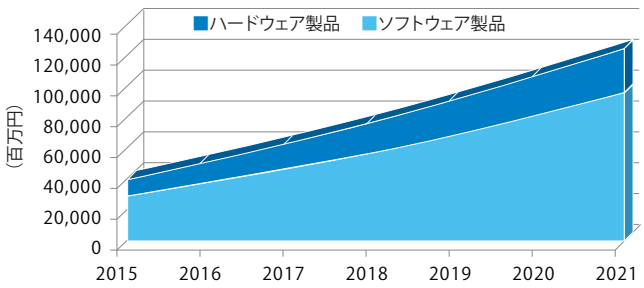


図-1 国内IoTセキュリティ市場 製品セグメント別 売上額予測、2015年～2021年(出典: IDC Japan, 2017年11月)

当社のお客様の間でも、セキュリティに対する経営者の意識はますます高まっています。ただ、サイバー攻撃の手口が多様化しており、意識はあってもどうすればいいのか、どういう製品でどのような対策ができるのか分からないというケースをよく耳にします。またセキュリティ製品は導入していても従来の製品では対応できないランサムウェアなどの新たな脅威も増加しています。

当社は、IT領域に対する標的型攻撃対策、改ざん検知、資産管理、クライアントセキュリティなどさまざまなセキュリティ対策製品やソリューションを提供していますが、海外のサイバーテロを例としたOT領域のセキュリティに関して話を聞く機会が増えており、早急にお客様のニーズに応えられる製品を提供していかねばならないと考えています**(図-2)**。

OT機器・システムを守る3つの製品

当社は、米国シリコンバレーで最新技術、最新製品を発掘するなど、セキュリティ製品や市場の調査を継続的に行っており、今後、次の3つの製品を当社のお客様に提供していけるよう準備を進めています。

(1) IoT機器への不正アクセスの自動検知

例えば、店舗などは監視カメラを設置して、店内の映像をサーバー側に蓄積し、何かあった場合に当時の映像を確認しています。このようなシステムにおいて、最近では外部からの不正アクセスによって監視カメラの設定情報が書き換えられ、ネットワークの経路を変えられて悪意のある不正サイトに映像が漏えいしたケースも見られます。

こうした脅威を検知するため、当社では、ネットワークのパケットを監視して不正なルートにアクセスしていないかをチェックする製品を準備しています**(図-3)**。機械学習を利用して通常の通信ルートを学習し、通常とは異なる経路で通信が発生した場合にアラート通知を行い、ネットワーク機器と連携して不正な経路

への通信を遮断する仕組みを提供します。

(2) 全体のアクセス経路を可視化

企業にはさまざまなネットワーク機器が存在しますが、すべてのネットワーク機器にアクセスして設定情報の取得を行い、アクセス経路のマップを作成、ネットワーク経路を可視化することができます。

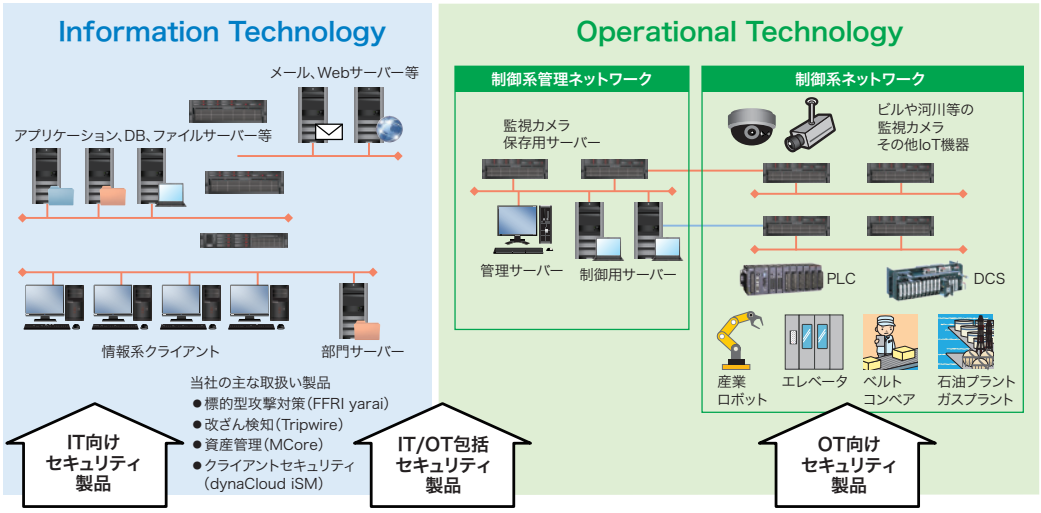


図-2　ITおよびOT領域

ネットワークの規模が大きくなると、機器の構成情報を1台ずつ管理するには大変な労力を要します。この製品を使えば、企業内のネットワーク全体が構成図として可視化され、設定した経路の正常性が一目で確認でき、PCI DSSなどのコンプライアンス・ポリシー準拠や監査対応が行えます。また、ネットワークの脆弱性リスクの検出と改善に向けた対応の優先度が把握できるようになります。

(3) ユーザーの行動分析を機械学習で監視

資産管理ソフトウェアの導入によってユーザーの操作ログなどさまざまなデータを収集できますが、これまでの操作ログは、情報漏えいの発覚後に誰がどのような操作をしたのか確認するために利用する場合が多く、通常は膨大なデータを保管しているだけでビッグデータとしての活用はしていない場合がほとんどです。本製品は、AD AUDITログ、アクセスログ、DBログ、メールログといったログを読み取り、機械学習を活用して、ユーザーの操作について行動分析を行うものです。日頃はUSBを利用しない人が突然ある日から大量のデータをUSBメモリに書き出している、普段アクセスしないサーバーに頻繁にアクセスし大量のファイルをダウンロードしている、といった予期せぬ行動をその場で検知することができます。

痒いところに手が届くセキュリティ製品を

当社のお客様にヒアリングをすると、「ソフトウェアのインストールが行えない製造ラインの機器に対してもエージェントレスのセキュリティ対策を行いたい」、「未知の脅威に対しても検知できる仕組みが欲しい」、「重要な個人情報を扱うシステムを外部攻撃から守りたい」といった声が聞かれます。前述した製品やソリューションを提供してニーズに応えることは急務となっており、研究開発に注力しているところです。

製造系のラインを持っているお客様においては、IT領域ではセキュリティ対策ができていても、それと切り離されている製造ラインでは手つかずの状態、というケースが少なくありません。当社では、IT領域向けのセキュリティに関しては多くのお客様に製品やソリューションを提供してきました。今後は、OT領域向けの商材も取り揃え、IoTセキュリティ市場に対して積極的に当社の技術力をアピールしながら、従来製品・ソリューションと合わせて拡販をしていきます。

(SIソリューション事業部　三ヶ月 一弘、渡邊 健一)

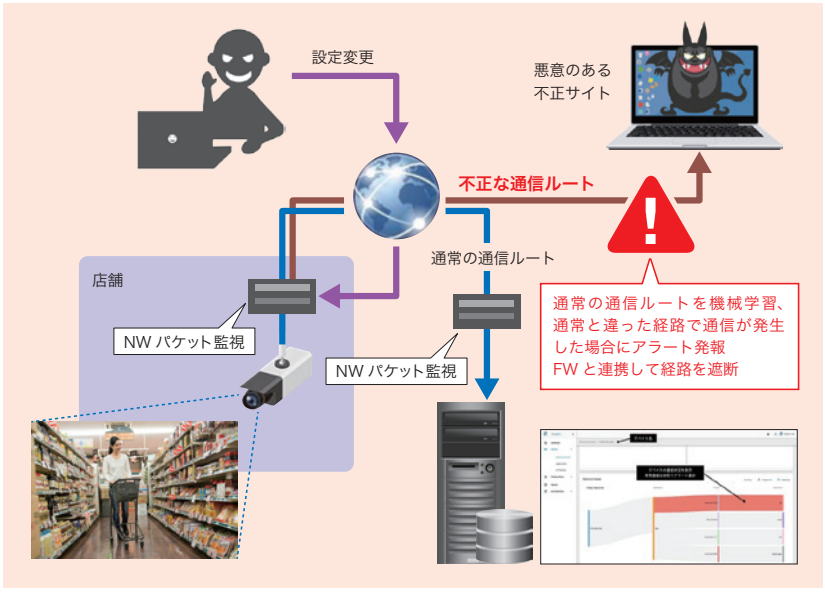


図-3　監視カメラへの不正アクセスの自動検知

セキュリティ対策機能を重視したクラウド対応統合資産管理サービスを提供

多くのIT資産管理ツールが存在する中、導入企業53,000社以上と高いシェアを誇るのが、「ISM CloudOne」です。IT資産の管理はもとよりセキュリティ対策に注力した点が特徴のクラウド型のサービスです。当社は「dynaCloud iSM powered by ISM CloudOne」として販売しており、手の甲静脈認証「VP-ⅡX」を用いた入退室管理システムと組み合わせることで、情報セキュリティの確保だけでなく勤怠管理としても活用でき適切な労務管理を実現します。

導入の容易なクラウド型のIT資産管理

ITの普及と活用の進化に伴い、企業を脅かすリスクも多様化しています。中でも、標的型攻撃による情報流出や内部不正による情報漏えいなど、個人情報・機密情報の漏えいによって企業が信用を失う事件をニュースなどで目にする機会は少なくありません。

当社が「dynaCloud iSM powered by ISM CloudOne」(以下dynaCloud iSM)として取り扱うクオリティソフト(株)の「ISM CloudOne」は、外部および内部のセキュリティ対策に重きを置いた統合IT資産管理サービスです。これまでの導入実績は53,000社を超え、マネージド型・クラウド型資産管理サービス市場では42%と圧倒的なシェアを誇っています(2015年:ミック経済研究所調べ)。

dynaCloud iSMは、IT資産管理ツールとして以下の機能を搭載しています。

1. ハードウェア・ソフトウェアの情報を自動で収集しレポート化する機能
2. ライセンス種別や形態、インストール状況などの詳細を表示するソフトウェアライセンス管理機能
3. 社内ネットワーク経由でソフトウェアやファイル、レジストリなどの配布・実行を行う機能
4. PCだけでなくスマートフォンやタブレットなども1つのコンソールで管理できるスマートデバイス管理

当社の提供するクラウド型のサービスのため、サーバー購入や管理は不要となり、すぐに運用を開始したい企業や専任の担当者がいない企業でも、迅速かつ低コストでの導入が可能です。あらゆる拠点、あらゆるデバイスの一括管理を、クラウドサービスを利用することで実現できます。

セキュリティの自動管理を実現

dynaCloud iSMは、前述したように資産管理ツールでありながら、セキュリティ対策に軸足を置いている点が他社製品との大きな違いです**(図-1)**。以下のようなセキュリティの外部および内部対策機能を備え、ダッシュボード(管理画面)でセキュリティレベルや状況をひと目で確認できます(一部オプション機能)。

(1) 自動脆弱性診断

対処が必要な端末が自動でレポート化されるため、運用工数を抑えたセキュリティ対策を実現します**(図-2)**。また、端末の状態とセキュリティ辞書[注1]を1日1回突き合わせることでPCの脆弱性を自動でレポート化、必要な是正操作をシームレスに行えます**(図-3)**。

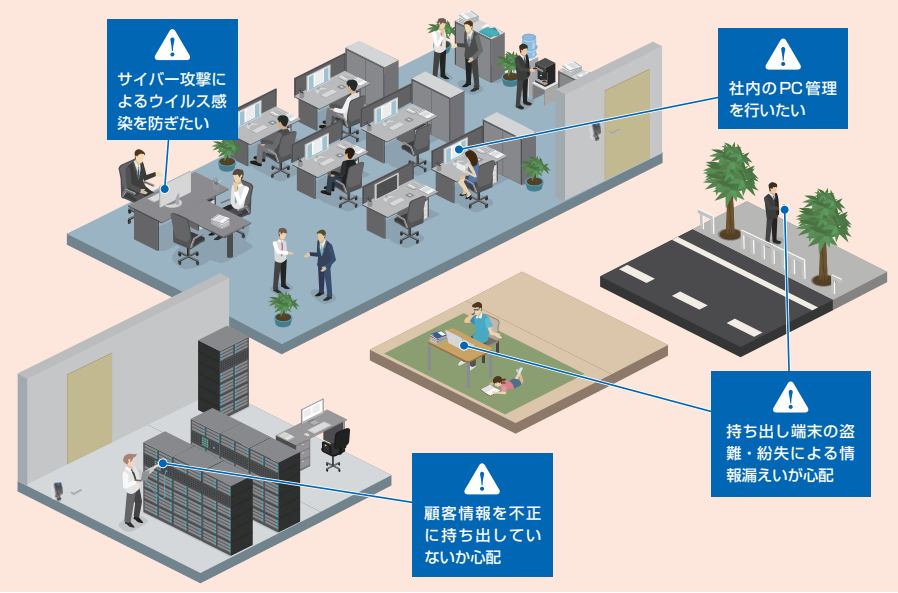


図-1 dynaCloud iSMによるセキュリティ対策

図-2　セキュリティの自動管理

(2) ふるまい検知

5つのエンジンでマルウェアを検知、静的＋動的分析で未知の脅威からPCを保護します。

(3) URLフィルタリング

不審なサイトの閲覧やストレージサービスへのアクセスを制限し、内部からの情報漏えいを未然に防止します。

(4) 禁止ソフトウェア起動制御

情報漏えいに繋がる恐れのあるソフトウェアリストのデータベースを搭載し、企業にリスクのあるソフトウェアの利用制御を簡単に行えます。

(5) 外部デバイス制御

USBメモリやCD/DVD、スマートデバイスなどの外部デバイス利用を制御し、ファイルの持ち出しによる情報漏えいを防ぎます。

(6) 操作ログ取得

クライアントPCの操作を見える化しログとして管理し、問題発生時の早期発見と不正操作を抑止します。

(7) ディスク暗号化

システム領域も含めハードディスク全体をまるごと暗号化し、端末内のファイルを守ります。

手の甲静脈認証を利用した入退室管理

最近では、指紋認証とパスワードといった、種類の異なる2つの情報を組み合わせることで安全性を高める二要素認証によるセキュリティ強化の必要性も話題となり、すでに自治体ではセキュリティ要件の1つとされています。民間企業においても個人情報・機密情報保護の観点から、あるいはプライバシーマークやISMSの取得・維持などで関心は高まっているものの、指紋認証システムなどの導入コストがネックになって二の足を踏むケースも少なくないようです。

ここにきて入退室管理などで採用が進んでいる手の甲静脈認証「VP-ⅡX」は、手の甲側の静脈パターンを読み取ることにより、季節などによる血管の収縮・拡張の影響も受けにくく安定した認証を行えるものです。生体認証のためICカード運用のような管理の手間がかからず、出入口など扉単位での機器構成のため、導入コストの点でも設置・移設などの柔軟性の点でもそのメリットが注目されています。

dynaCloud iSMはVP-ⅡXと連携することで、情報の漏えい防止やセキュリティエリアの入退室管理など強固な情報セキュリティの確保を実現する環境を提供します。オフィス入室時の静脈認証を行う際には、4桁のワンタイムパスワードが発行されます。入室後にはそのパスワードを入力してPCにログインする仕組みのため、権限のない第三者や未入室のユーザーがPCにログインすることはできません。また、従業員の入退室情報とPC稼動ログと連動することで勤務実態の把握が可能で、従業員の勤怠管理などを行えるメリットもあります。例えば、PC稼働状況のログと実際の出退勤の状況には大きな差分が生じるケースもあり、そのような場合でも従業員の勤務実績をもとに効率化対策を講じることができます。働き方改革が声高に叫ばれている中、dynaCloud iSMとVP-ⅡXを組み合わせることで、適切かつ効率的な労務管理に取り組むことが可能となります。

dynaCloud iSMは当社のクラウド基盤を使ったクラウドサービスとして展開しており、お客様の導入コストを抑えながら、1つのソリューションで企業が必要とするセキュリティ対策とIT資産管理を提供しています。今後もお客様のニーズを満たすセキュリティソリューションを実現していきます。

（SIソリューション事業部　藤井 文治）

注1）セキュリティ辞書：Windows更新プログラム、Adobe製品、Java、ウイルス対策ソフト、Webブラウザなどのあるべき姿（最新状態）が登録されたデータベース。辞書は毎日更新されます。

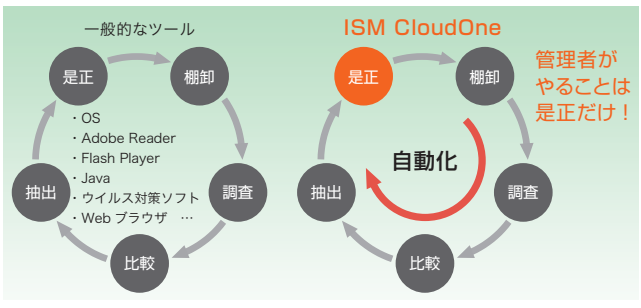


図-3　脆弱性対策工数を大幅に削減

機密情報の流出を自動で「探して」「守る」情報漏えい対策ソリューション

当社は、個人情報などの重要・機密情報ファイルを見つけて自動で暗号化するソリューション「Secure Protection（セキュアプロテクション）」を販売しています。釧路市では、自治体情報システムのセキュリティ対策強化に本製品を導入し、職員の負担がほとんどない運用で情報流出・紛失への対策を実現しています。

「情報は流出すること」を前提としたソリューション

多くの企業では、ウイルス対策はもとより、重要・機密ファイルの持ち出し制限、USBメモリなどの持ち込み・使用の禁止、従業員のセキュリティ教育、機密保持誓約書など、さまざまな対策を講じてきました。にもかかわらず、情報流出事件・事故は毎日のように起きており、従来の「流出・漏えいを未然に防ぐ」ツールの導入だけでは、情報流出は防ぎ切れないのが実情です。そうであれば、「情報は流出する」ことを前提とした対策を講じるほかありません。

当社が販売している「Secure Protection」は、まさに「情報が流出しても漏えいはしない」ことをコンセプトにした製品です。守るべき情報を探し、暗号化し、管理・追跡し、万一の流出の際にはファイルをあとから消去する、という一連の動作を自動的に実行することで、あらゆる経路での情報流出や紛失を抑止するものです**（図-1）**。

(1) 自動で「検索」「暗号化」

あらかじめ指定したルールで社員のパソコンを定期的に検索、独自アルゴリズムで個人情報を含む重要・機密ファイルを高精度で検出します。マイナンバー、住所、氏名、電話番号、メールアドレス、口座番号、クレジットカード番号、免許証番号、保険証番号などを含むファイルの検索を行うほか、重要、極秘、文書番号などあらかじめ設定したキーワードによる検索も可能です。

また、検索により検出されたファイルは、自動的に暗号化されます。

(2)「管理・追跡」と「あとから消す」

暗号化した重要・機密情報ファイルは、リアルタイムでファイルへのアクセス・操作ログを確認でき、いつ誰がアクセスしたかが追跡できます。万一、ファイルが流出した場合でも、「あとから消す」仕組みにより、情報漏えいを防ぎます。検索・暗号化したファイルの閲覧制限は管理サーバー上で一元管理され、閲覧制限の変更が可能です。

釧路市が2,000ライセンスを導入

釧路市では、2016年2月にこのSecure Protectionを全職員の端末に導入し、情報セキュリティ対策の強化に成功しています。

導入当初は、マイナンバー制度の運用開始を控え、全国の自治体情報システムのセキュリティ強化が求められました。同市では早くから、USBメモリなど外付けデバイスの制限や使用状況のログを残す仕組みの導入、さらには業務システムのインターネットからの分離、メールの無害化などに取り組んできました。個人情報を含むファイルについても、各職員のPCには個人情報は残さずサーバー上に保管するということも徹底してきましたが、消去忘れなどヒューマンエラーによる情報流出のリスクは残されていました。

同市では、万一ファイルが外部に流出したとしても、そのファイルが開けなければ事故には結びつかないと

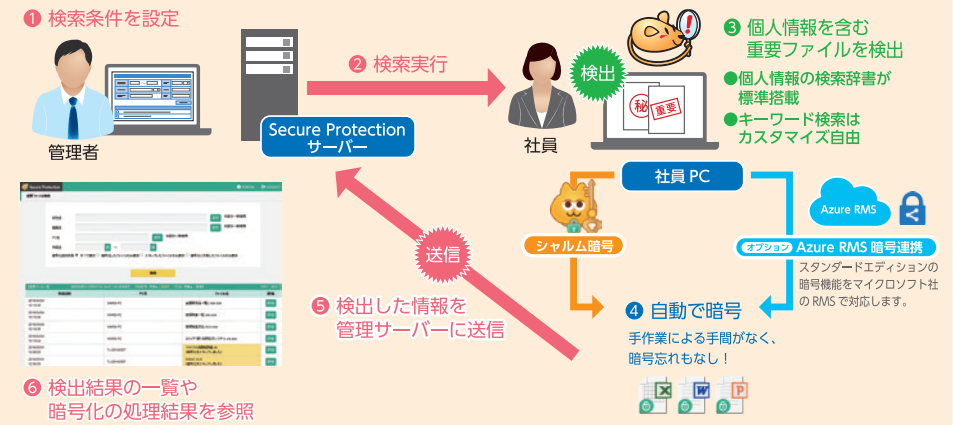


図-1　Secure Protectionの概要

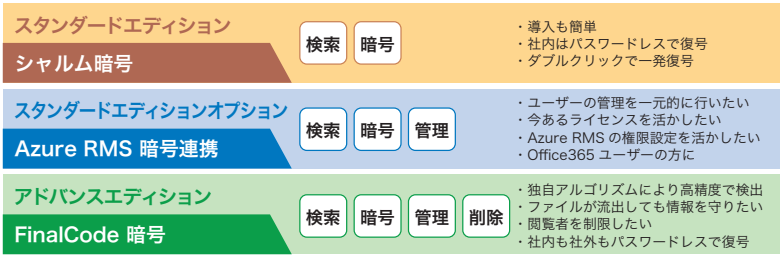


図-2　選べる暗号化方式

いう対策を講じるほうが合理的・現実的だと考え、職員の負担が極力少なくファイルを暗号化するツールの検討を始めました。

選定のポイントとなったのは、以下の3点です。

1) 職員が特別の操作をしなくても暗号化できること

2) 暗号化するファイルの選定条件を自由に設定できること

3) 適正な費用で導入できること

以上のポイントから、最終的にSecure Protectionを選定し、2,000ライセンスを導入しました。

一般競争入札からSecure Protectionの運用開始まではわずか3カ月。百数十の部署から各部門のセキュリティの担当者が参加、わずか2時間の説明で導入準備は完了したのです。

Secure Protectionは自動的に暗号化できる点が最大の特長で、ユーザーが意識することなく暗号化されるため、従来と使い勝手はほとんど変わらず、職員の負担が少ないツールを検討したいという同市のニーズに応えることができました。

運用開始直後は、すべてのファイルに対して検索を行い、対象ファイルを暗号化するため、釧路市ではPCに負荷がかかるのではないかという不安もあったようです。そこで、初回のみ、職員が業務を行わない夜間にファイル検索を行うことで対応、2回目以降は差分検査を行うため、業務に支障が出るような負荷はありませんでした。現在は、昼休みの時間帯を利用してファイル検査・暗号化を実行しています。これにより、守られているという安心感を持っていただきました。

Secure Protectionは、名字、住所、生年月日、マイナンバー、口座番号などの個人情報の検索辞書を搭載しており、ファイルの検出レベルをお客様側のニーズに合わせた形で調整可能です。当社は、ファイルを暗号化する基準をさらに厳しくしたいという同市の要望にも対応しています。

「Microsoft Azure RMS」を追加サポート

2017年4月、Secure Protectionに新たな暗号化方式を追加しました。従来のシャルム暗号(スタンダードエディション)とFinalCode暗号(アドバンスエディション)に加え、Microsoft Azureのクラウド用オプションとして「Azure RMS暗号連携（スタンダードエディションオプション)」を提供しています**(図-2)**。

Office 365 環境でも情報漏えい対策を強化したいといったニーズに対応した機能で、新たに暗号化環境を用意することなく、Secure Protectionによる情報漏えい対策を導入できます。Secure Protection で検索した電子ファイルは Microsoft Azure RMS で暗号化され、情報漏えい対策の強化を図ることができます。本機能は、スタンダードエディションにわずかなオプション費用で利用できます。

このほか、「デバイス制御オプション」も新たに用意、基本機能に加えて、ファイルの不要な持ち出し、標的型攻撃などによる流出などのインシデントに対する対策を強化することができます**(図-3)**。各種デバイスへの機密情報ファイルの移動やコピーを禁止する「デバイス制御機能」や、ファイル操作ログ、メール送信ログ、印刷ログを取得して管理する「ログ管理機能」を搭載しています。

Secure Protectionは、金融から建築までさまざまな業種のお客様に導入いただいています。当社のWebサイトにも、さまざまな業種や規模の企業から問い合わせをいただいています。個人情報は守りたいが、人間が介在する以上、守り切れない、万一流出しても漏えいはしない、しかも情報システム部門や利用者が従来の仕組みを変えないで実現できる、という点で多くの企業が関心を示しています。

文部科学省では2017年秋に「教育情報セキュリティポリシーに関するガイドライン」を策定し、今後は、学校や教育機関などでもセキュリティ対策強化が求められてくるものと考えられます。こうした文教市場も含め、少しでも多くのお客様に製品のメリットを訴求していきます。

(SIソリューション事業部　山本 崇史)

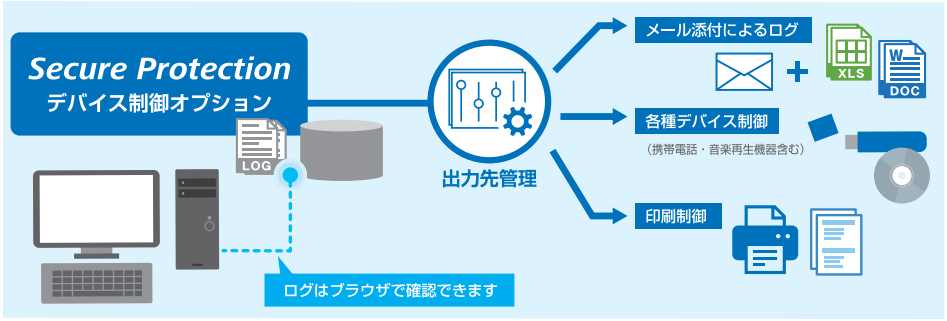


図-3　デバイス制御オプション

改ざん検知やコードの難読化で組込み機器のソフトウェアを保護

IoTの進展によって組込み機器市場が裾野にまで拡がり、ネットワーク接続も進むことで、サイバー攻撃などのリスクが顕在化しています。これらのリスクに対応するためには、改ざん検知やコードの難読化のように、ソフトウェア自体を保護することが対策として挙げられます。当社は、実績のあるソフトウェアプロテクション・ツールを提供してこれらのニーズに応えます。

ソフトウェアへの脅威に対処

社会の至るところで組込み機器が活躍するようになるとともに、それに対するセキュリティリスクも高まってきています。さらに、組込み機器のネットワーク接続が進み、個人が特定されるなどの多様な情報を頻繁に扱うようになったことで、そのリスクは拡大する一方です。

これらのリスクに対応するためには、攻撃の入口となるネットワークへのセキュリティ対策はもちろん必要ですが、機器で動作するソフトウェア自体の保護も考えていかねばなりません。自動車の制御を行う車載ソフトウェアでは、その処理内容を悪意により書き換えられる可能性があり、最悪の場合には、重大な事故につながる可能性があります。また、カード情報を扱う機器のソフトウェア内に暗号鍵やパスワードの情報が記録されていれば、その情報を解析されてカード情報の漏えいが発生し、金銭的な被害にも繋がります。

こうした脅威から組込み機器のソフトウェアを保護するため、当社では、セキュリティ機能を実装する受託開発はもちろん、セキュリティソフトウェアIPやツールの販売、脆弱性管理に関するコンサルティングや教育など、さまざまな取り組みを行っています。

ここでは、これらの取り組みのひとつとして、当社で販売しているインサイドセキュア社のソフトウェアプロテクション・ツールについて紹介します。

改ざんや情報漏えいから機器を守る3つの機能

本ツールは、「Core」と「WhiteBox」という2つの製品から構成され、「実行時の改ざんチェック」、「コードの難読化」、「機密情報の秘匿」の3つの機能を提供します。

(1) 実行時の改ざんチェック(Core)

ソフトウェア実行時に不正な改造が行われていないか、チェックを行う機能です。ソフトウェアを構成しているいくつかの関数にチェック処理を埋め込み、実行中に動的に改ざんの有無を確認します。ソフトウェアの各所に埋め込まれたチェック処理が、各エリアを相互に監視することで全領域の安全性を確実にチェックすることが可能です**(図-1)**。

このようなチェックの方法では、チェック処理の埋め込み量が多過ぎると処理速度の低下に、少な過ぎるとチェック漏れにつながります。つまり、チェック処理の量(安全性)とパフォーマンスはトレードオフの関係にあります。本製品以外にも実行時の改ざんチェック機能を持ったツールは存在しますが、チェック処理の埋め込み箇所やその量は、開発者の経験によって決める必要があります。しかし、本ツールは、ソフトウェアの実行時のデータを取得して自動分析する機能を備えているため、パフォーマンスを低下させずに十分な安全性を確保する最適な配置を自動で行ってくれます。

(2) コードの難読化(Core)

プログラムの流れを複雑にし、攻撃者による不正なソフトウェアの解析を困難にする機能です。例えば、ソフトウェアの中で条件分岐する選択肢の数や、ループの多さなどは、攻撃者がプログラムのバイナリを解析する際の大きな手がかりとなります。コードの難読化機能では、条件式の複雑化や、ループなどの制御構造の変更、ダミーコードの挿入などを組み合わせることで、プログラムの複雑度を増加させます。

難読化の度合いは細かくチューニングでき、性能要件への適合、コードサイズの制限に対応します。処理速度を極力落とさずリバー

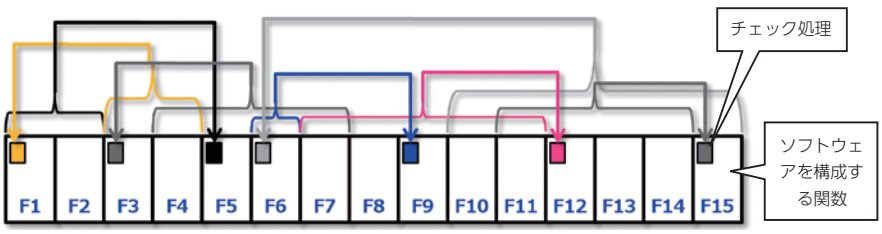


図-1　改ざんチェックの仕組み（複数のチェック処理で相互監視）

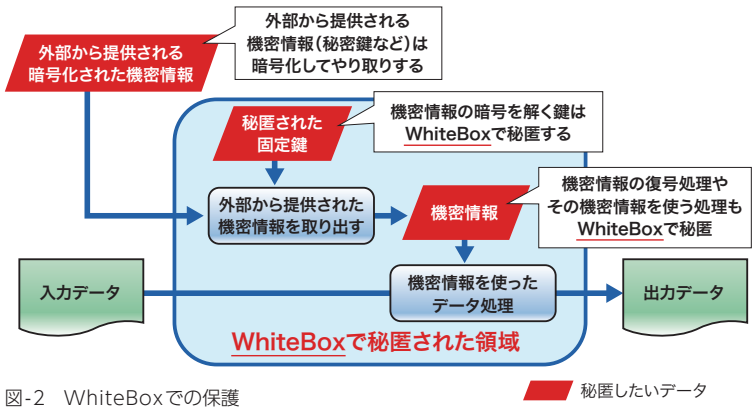


図-2　WhiteBoxでの保護

スエンジニアリングを阻止したい場合に最適な機能と言えます。

(3) 機密情報の秘匿(WhiteBox)

ソフトウェアに埋め込まれた機密情報を強力に秘匿する機能です。例えば、どんなに強力な暗号アルゴリズムを採用しても、その暗号処理を行っているソフトウェアを動的に解析されれば簡単に暗号鍵を取り出されてしまいます。しかし、この秘匿機能を使用すれば、もし攻撃者が動的に解析を行ってソフトウェアの中身を見たとしても、暗号鍵などの機密情報は確実に秘匿され、まったく別のソースコードに変換してくれます。

図-2のように、外部とやり取りする機密情報は暗号化し、それを解く鍵や復号処理をこの機能で秘匿することで、動的解析をされたとしても安全なソフトウェアを実装することが可能です。処理速度の低下やサイズの増加を伴っても、機密情報を守らねばならない場合には最適な機能です。この秘匿処理は関数ごとに適用できるため、絶対に秘匿したい部分に絞って使うことで、影響を最小限に留めることが可能です。

開発環境と統合し2つのフェーズで保護

本ツールは、開発環境の中に統合されます。ツールにより自動的に解析コードと保護コードが挿入され、ソースコードの修正は特別なカスタマイズが必要な場合を除き不要です。

まず第1フェーズである「分析ビルド」では、ソフトウェアの実行時のデータを収集するための機能を埋め込んだ形で一度ソフトウェアを生成します。コンパイルしてソフトウェアが出来上がってから実行し、その動作情報をデータベース化していきます。その後、第2フェーズの「保護ビルド」でデータベース内の動作情報を使って最適な場所にチェック処理を埋め込むことでソフトウェアが完成するイメージです**(図-3)**。

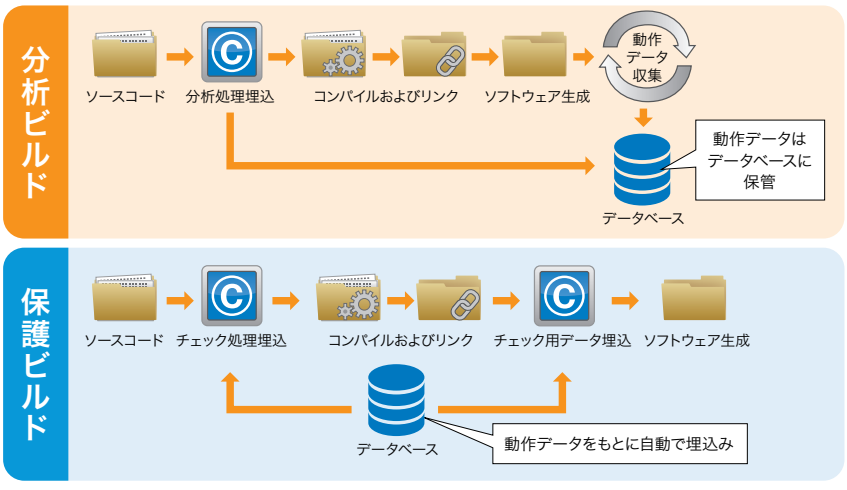


図-3　2つのフェーズで保護

これまで説明した機能を使用して、ソフトウェアを強力に保護しようというのが、当社が提供するソフトウェアプロテクション・ツールです。「鍵の管理は専用のチップ(TPM)を導入しているのでWhiteBoxの機能は必要ない」というお客様や、「ソフトウェアの処理は特殊なことはしていないため難読化は必要ない」といったお客様は、改ざん検知機能のみでも利用可能です。ソフトウェアのアップデート用のアクセス先のURLを書き換えられてしまう、TLS通信用の認証局の証明書に不正なものを追加されてしまう、データを外部に不正に送信する機能が追加されてしまう、といったリスクを防ぐことができます。

IoT時代が到来し、各所にセンサーが配備されるようになってきました。公の目に触れるところで使われながらもセキュリティ監視されていないセンサーや機器が脅威にさらされる危険性が高まり、これらで動作するソフトウェアをいかに保護するかは、今後ますます重要な課題となってくると思われます。

Core/WhiteBoxは、すでにスマートフォンのカード決済アプリケーションをはじめ、モバイル機器やオフィス機器などを扱う情報機器メーカーを中心に豊富な導入実績があります。IoTの進展に伴い、センサー機器にも活用されていくと期待しています。

当社は、本ツールの販売、アプリケーション開発のお手伝いはもちろんのこと、ツールのコンサルティングから教育までを含めたトータルなサポートを提供していきながら、車載などの新しい分野にも拡販していきたいと考えています。

(エンベデッドシステム事業部　関根 正騎)

機械学習を使ったLSI検証への取り組み

肥大化する検証量への対処を目指して

最近のIT関連技術は、AIやビッグデータ処理などといったキーワードを抜きには語れないほどになってきました。それは、計算機の処理能力向上とIoT技術の急速な普及により、利用可能なデータが増え続け、その種類や形態も多様化していることに起因します。

この大容量かつ複雑化したデータを分析する手法の一つに「機械学習」があります。機械学習は、データを解析した結果を基に、データを分類する、データパターンを見つける、モデリングにより結果を予測する、といったことを可能にします。つまり、データがあるところに、機械学習を活用した第四次産業革命のビジネスチャンスがあるわけです。

当社では、この機械学習をシステムLSI設計・検証に活用するため、研究開発への取り組みを進めています。

LSI設計は年々、大規模化かつ複雑化していますが、大量の検証結果のデータ解析を人間がカバーできる範囲は限られます。LSIの仕様はより複雑さが増し、多くのオプション機能を内部に実装します。それに伴い、検証項目は増大し、その組み合わせも膨大なものとなります。今までの手法では、回路の成熟度に合わせテストパターンを増やしながら検証していましたが、これには多くの時間と人数が必要となってしまいます。残念ながら大量のデータを有効活用して解析を進める、という流れには至っていないのが実情です。

そこで、機械学習を活用して人間が優先的に行うべきものを指南してくれるような仕組みを作ることで、効率よく対処できないかと考えました。

LSI開発全体に成果の活用を

現状のLSI検証では、事前に決定した優先度に基づき解析を行い、バグの可能性のあるものを設計者にフィードバックする、というサイクルを回していますが、これが最良の方策とは言えません。研究開発では、検証データのエラー結果から対象回路の入力信号や設定状況の共通性を抽出し、エラーとなる要因を種類ごとに提示するシステムを構築しました。これにより、どれくらいエラーの要因がありそうか、どの検証パターンを先に対処すればエラー数の収束が早まるか、という戦略を立てて検証を行えます。そして、人間が無作為に作業を進めていく方法と比較し、高効率化や未知のリスクの回避が期待できます。

このシステムでは、機械学習のベースとなるアルゴリズムのうち「クラスタリング（教師なし学習）」と「パターンマイニング（教師あり学習）」を用います。クラスタリングは、無秩序にある結果を持たないデータから特徴を導き分類します。パターンマイニングは、例えばP（Pass）あるいはF（Fail）といった結果を持ったデータ群から、結果を予測するモデルを作ります（**図**）。

LSI検証のエラー結果を解析するこの取り組みは、検証パターンの要因分析や分類だけにとどまりません。例えば、エラーの要因を導き出してくれるなど人間の手ではできない、さまざまな副次効果も期待できます。

LSI部門では、知識や経験の少ない機械学習を、LSI設計・検証に活かすことは容易ではありません。そのため、データ解析や機械学習で先行しているSI部門との連携により、研究開発を進めています。今回の取り組みで得られる知見を、LSI開発に広く活かしていきたいと考えています。

（LSIソリューション事業部　鈴木 孝洋）

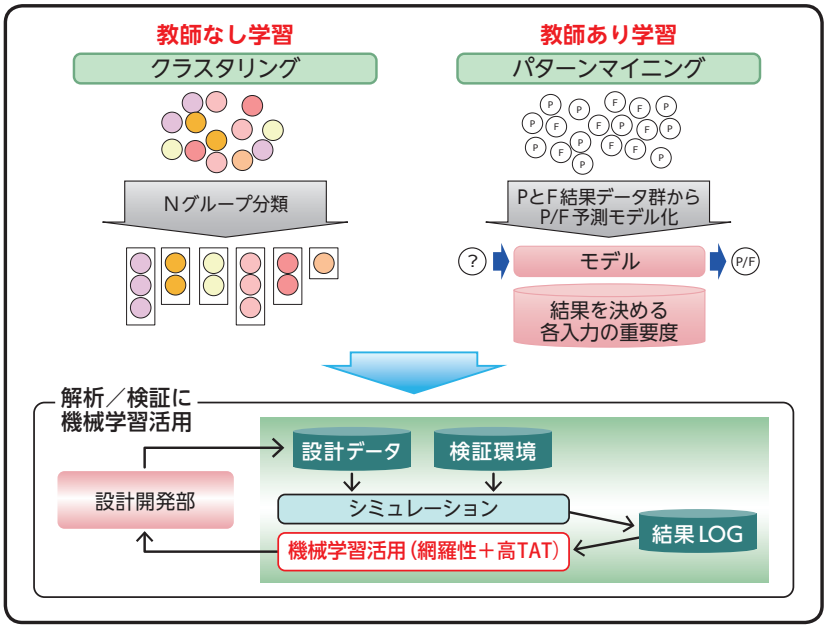
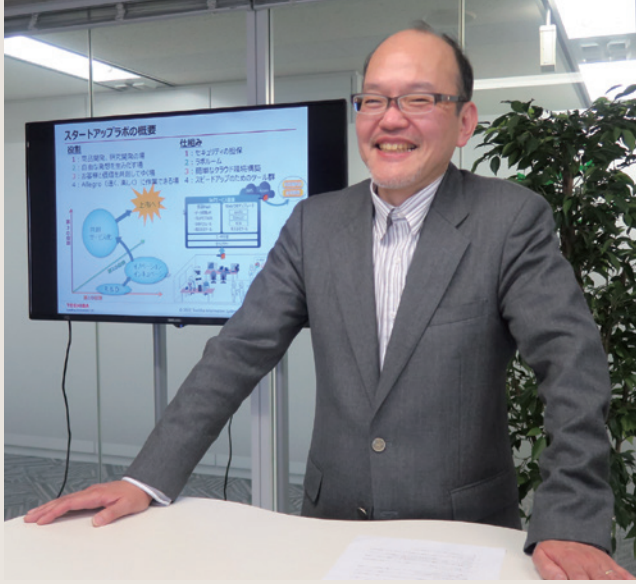


図　検証解析用機械学習システム

PERSON
［人］

技術マーケティング部
マーケティング・商品企画担当 参事
中屋　和之



スタートアップラボでお客様と共に新しい価値の創造を

お客様とのビジネス共創を推進するラボ

入社して約30年、当初は組込みシステム開発に従事し、人工衛星との通信プログラムや自動車のエンジン制御、自動券売機に至るまで、さまざまな機器の制御プログラムを開発してきました。その後、Webアプリケーションの開発にも携わり、現在は、エッジデバイスからのデータを蓄積・分析するIoTサービス基盤をクラウド上に構築する研究開発に取り組んでいます。

当社は、2017年夏に、IoTサービスをはじめとした事業ドメインを横断する融合商品創出を目的として「スタートアップラボ」を開設しました。次の4つを役割としています。

(1) 研究開発や商品開発、サービス試行が簡単に行える場
(2) 事業の垣根を越えて自由な発想でイノベーションを生む交流の場
(3) クラウド上でお客様とセキュアに繋がり、付加価値の共創ができる場
(4) Allegro（速く、楽しく）に作業でき、新規事業創出ができる場

こうした役割を果たすため、ラボではマルチクラウド環境を整え、IoTサービス基盤を利用し、各種エッジデバイスを接続して容易に製品・サービスの試行ができる場にしています。自由の中にも一定の節度を保つための強固なセキュリティ、ちょっとした思い付きやアイデアを形にするなど自由な発想ができるよう配慮した作業空間、クラウド上でお客様と共創する環境を容易に構築・運用できるインフラ、開発のスピードアップや工数削減を図る各種ツールといった仕組みを用意するなど、今まで当社になかった作業環境を実現しています。


ユニークなデスクやチェアを揃えたラボ室内

知識と経験をラボに最大限に活かして

ラボ内は、複数の大手クラウドサービスと直接接続しているほか、キャリア網を利用したVPN接続も使えます。また、お客様も安心して利用できるセキュリティを担保した環境を特徴としています。現在は、それぞれの業務に応じて、例えば3Dプリンターで作成した試作デバイスの動作検証を行ったり、クラウドサービスを試したり、といった使われ方をしています。さらには、こうした研究開発利用だけにとどまらず、お客様との共創目的で、互いのラボ環境を相互接続する仕組みを構築する取り組みも行われています。

ラボを運用するためには、私自身もクラウド、ネットワーク、セキュリティなどの技術に精通していることが不可欠だと考えています。過去の業務で得た知識、培ってきた経験を活かすことはもちろん、当社の専門知識を持つ有識者の協力を得てレベルアップに努め、お客様や社内のメンバーが安心して利用できるラボにすることが役割であると気を引き締めています。このほか、利用者の座り心地を考慮した椅子を導入するなど、新しい経験も楽しくさせていただいています。

今後は、クラウド上でのサービス展開が当たり前となり、さらなる短期開発も求められてくるでしょう。ラボはそうしたお客様や社内の要求に応えるべく、マルチクラウド化したプラットフォームをベースに、より簡単かつ素早いサービス展開ができるよう、進化を続けていかねばなりません。このスタートアップラボに、LSI設計から組込み、Web開発まで、当社の高い技術力を集結させ、お客様との新しい価値創造に邁進できるよう支援していきます。

Wave
Vol.23　2018年5月7日発行
発行人：長田　茂
発　行：東芝情報システム株式会社
〒210-8540 川崎市川崎区日進町1番地53（興和川崎東口ビル）
連絡先：技術マーケティング部
E-mail wave@tjsys.co.jp　URL https://www.tjsys.co.jp/

TOSHIBA
Leading Innovation

dynaCloud iSMの新機能
VP-II XとISMの連携

product

PCログイン認証と連動
（オプション）

入室時の静脈認証でランダムなOTPを発行。
権限のない第三者や未入室のユーザはPCにログインできません。

「適切な労務管理」と「情報セキュリティの確保」の両立を
プロダクト+BPOサービスにて実現

BPO

勤怠管理としての活用

管理コンソールから入退室履歴を管理できるため、タイムカード代わりとしての活用が可能です。

ism CloudOne との連携で残業問題へ対応！

PC稼働ログと連動することで、勤務実態の把握が可能。適切な労務管理が行えます。

東芝情報システム株式会社

SIソリューション事業部
〒210-8540 川崎市川崎区日進町１番地 53（興和川崎東口ビル）
TEL: 044-246-8670（ダイヤルイン）
E-mail:si_sales@tjsys.co.jp https://www.tjsys.co.jp/