増え続けるオペレーションコストの問題を解決し，被害を極小化する技術の確立と展開

古賀 祐匠　中嶋 良彰
千葉 直子　三好 潤
小山 高明　司東 秀浩
宮島 麻美
NTTセキュアプラットフォーム研究所

サイバー攻撃等の新たなサイバーセキュリティの脅威に対応しつつ，そのオペレーションを自律化・自動化する技術の確立によって抜本的に効率化します．オペレータが機械的には対応できない高度な脅威に関する対策により専念できるようにし，総合的なセキュリティ対応力の強化を図ります．

背　景

サイバー攻撃は年々増加しており，加えてその手法は複雑化・巧妙化しています．特に「人」をねらうサイバー攻撃の増加が著しく，それに伴って企業のセキュリティ対策費は増大を余儀なくされています．

ユーザの価値観が多様化し，ロングテールへの対応が必要な将来，さまざまな通信機器や端末・デバイスが接続された超高速光通信ネットワーク上では，サーバやソフトウェアが連携して多種多様なアプリケーションが提供されることが想定されます．そのような環境では，サイバー攻撃が発生する都度行うかたちの対策ではコスト効率があまりにも悪く，企業のデジタルトランスフォーメーションやビジネス価値創出を妨げる要因にもなり得ます．

本研究開発の目標

本研究開発では，サイバー攻撃やそのターゲットとなるさまざまな脆弱性に対して，常に先回りして自動的にセキュリティ対策を実施可能にすることをめざしています．

サイバー攻撃による被害発生を回避し，企業の経営を圧迫するセキュリティオペレーションの人的リソース不足の問題を解消するとともに，ユーザが安心して価値を享受できるICT環境を提供します．このような環境が，企業をセキュリティ脆弱性等の都度対応（もぐらたたき），インシデント発生時の後追い対応（いたちごっこ），そして被害によって生じるビジネス損失から解放します．

セキュリティオペレーションにかかるトータルコストの軽減によって，企業がサービスの「開発」や「運用」に集中できる状況をつくり出し，Smart Worldにおいてビジネス価値を短いサイクルで繰り返し創出し続けられるようにサポートします．

本研究開発が実現する基盤のイメージ

セキュリティオペレーションの現場では，「監視」「分析」「対処」の多くのセキュリティ対策を人手によって実施しているため，その対応力は人的リソースに深く依存しています．

本研究開発では，インフラやサービスを構成する機器やアプリケーションの状態を常に監視し，脆弱な状況を見つけ次第，先回りしてサービスやインフラを構成するシステムにセキュリティ対策を自動実行する基盤を実現することによって，効果的かつ効率的なセキュリティ対応を安定実施可能にします（**図1**）．

基盤の実現に向けた課題

常に先回りしてセキュリティ対策を自動実行するために，以下の3つの技術の確立をめざす研究開発に取り組むとともに，これらの研究開発を通じて**図2**に示すインテリジェンスを創出していきます．

(1)　脆弱性の積極的な可視化・最小化と自動修正サイクルを実現する技術

脆弱性の積極的な可視化・最小化と自動修正サイクルの実現により，セ

キュリティ対策のシフトレフトを可能にして強固なセキュリティを提供します．

⑵　環境変化に追随するインテリジェンスを創出・活用する技術

通信キャリアならではのインテリジェンスを自動生成するとともに，インテリジェンスを意識する必要のない自動活用技術によって，多種多様なICT環境に継続的・自律的にセキュリティ対策を実施します．

⑶　ヒトに起因するリスクを対策する技術

ヒトに起因するリスクに対応可能なセキュリティ技術を確立し，セキュリティ被害につながるヒューマンエラー，ヒトをねらう詐欺攻撃，および従業員等による内部不正行為等に関するリス

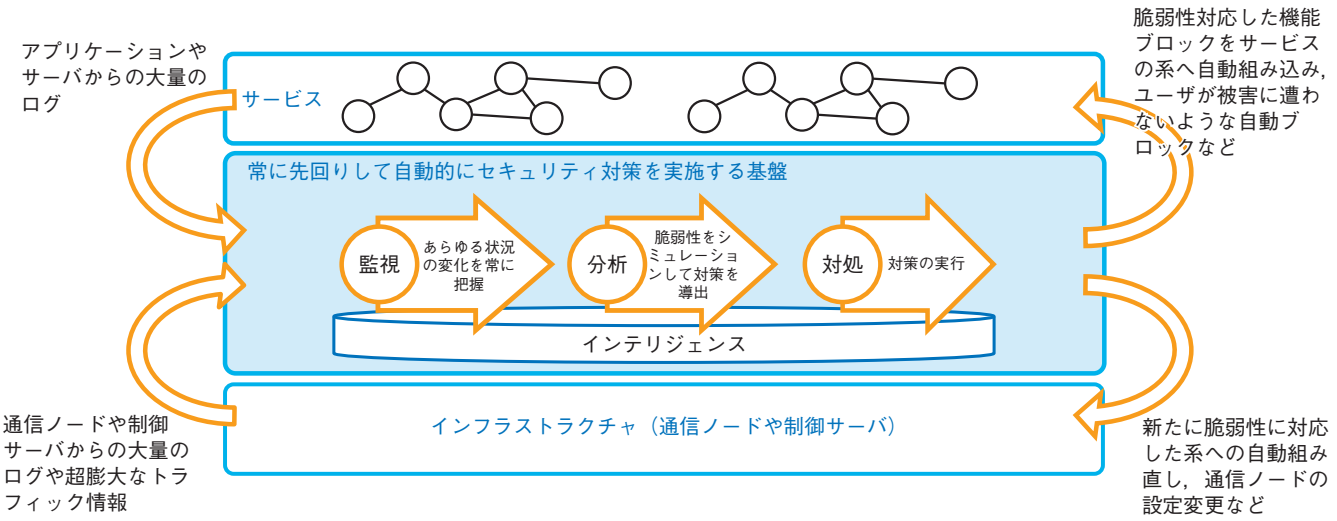

図１　本研究開発で取り組む基盤のイメージ

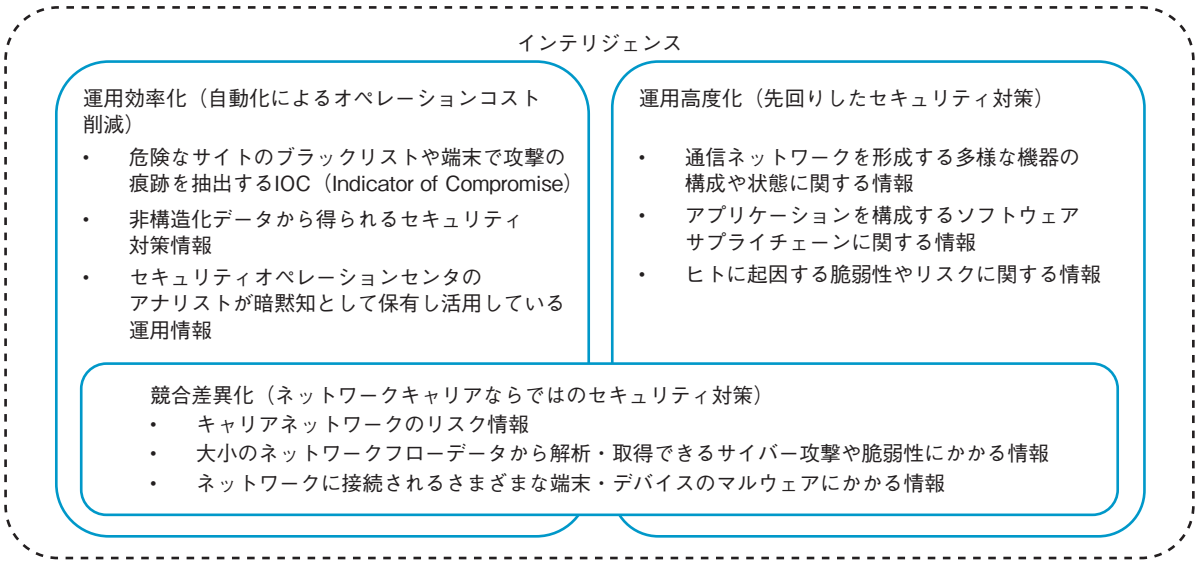

図２　本研究開発で創出するインテリジェンス

クを抜本的に低減します．

以降では，上記の研究開発に関して，現在の代表的な取り組みを紹介します．

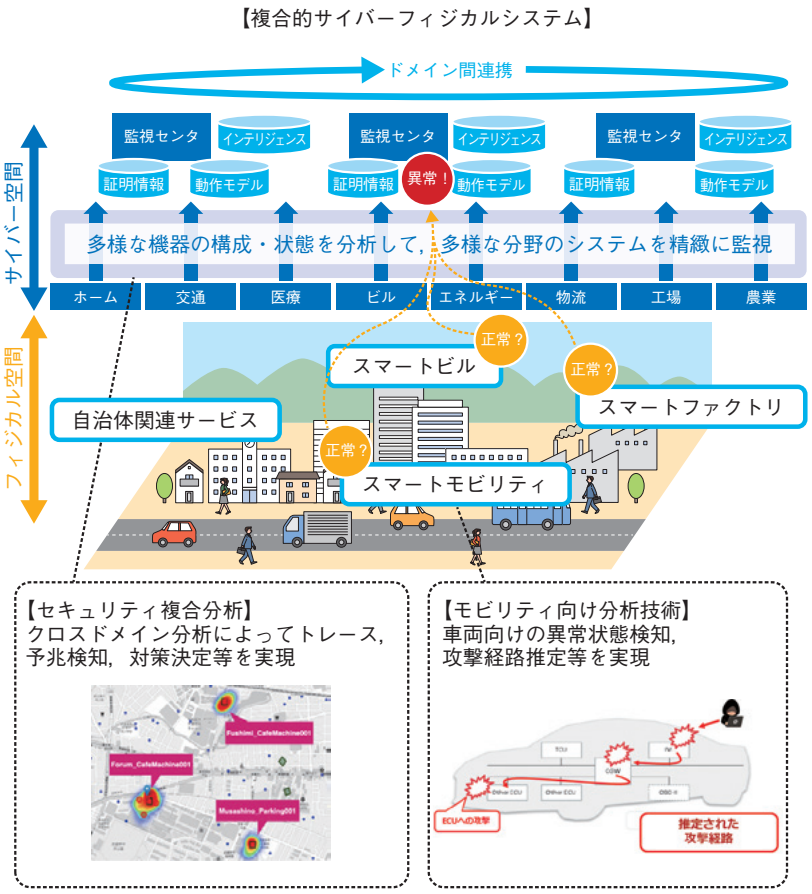

図 3　構成・状態分析技術

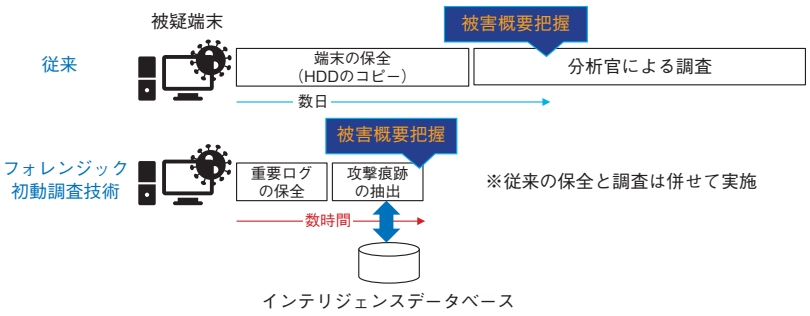

図 4　フォレンジック初動調査技術

現在の取り組み

⑴　構成・状態分析技術

スマートシティのような多様な要素によって構成される複合的サイバーフィジカルシステムを守るセキュリティ対策技術として，現在，ヒトやモノの構成・状態を分析するエージェントと通信解析エンジンの研究開発を行っています．今後は，構成・状態に加えてシステムやサービスをまたいだ要素間の関係性もとらえ，従来は困難であったセキュリティ異常の予兆検知，原因推定を行うクロスドメイン分析技術の研究開発を行っていきます（**図 3**）．

⑵　フォレンジック初動調査技術

一般的にフォレンジック調査では，被疑端末を保全し，分析官が攻撃の痕跡を抽出します．この調査は詳細な分析が可能な一方，分析官の経験に依存しており，期間は数日にわたることから，いち早く被害概要を把握する初動調査のフェーズで正確性・迅速性に課題が残ります．そこで，重要なログのみを保全し，攻撃の痕跡を自動的に抽出できる技術の開発に取り組んでいます．この技術は，攻撃者がよく使う攻撃の流れをインテリジェンスとしてデータベース化し機械的な処理を通して，分析官の習熟度によらず，数時間で初動調査ができることをめざしています（**図 4**）．

⑶　ヒトの心理や弱みをねらったソーシャルエンジニアリング攻撃検出技術

世界的なスポーツイベントの開催や

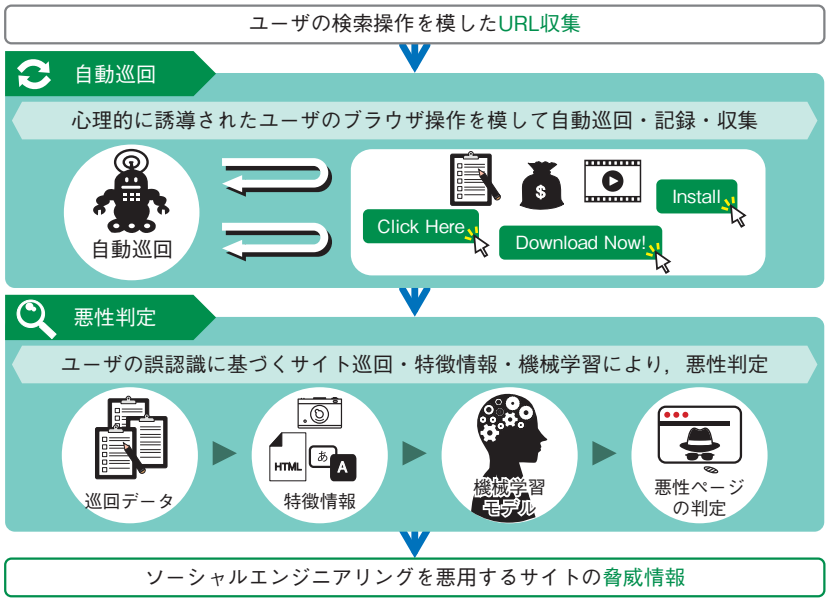

図5　ヒトの心理や弱みをねらったソーシャルエンジニアリング攻撃検出技術

新型コロナウイルス感染症の流行に伴い，人々の好奇心・恐怖心等を悪用したサイバー攻撃の被害が非常に増えています．攻撃者は，人の興味関心をひくコンテンツや偽の警告画面などにより，利用者を悪性サイトへ巧みに誘導し，マルウェア感染や金銭・個人情報の窃取を引き起こします．この取り組みでは，そのような人をねらった詐欺被害等を低減させることを目的に，騙される人のブラウザ操作をエミュレートして，Webページを自動で巡回・収集し，画像や言語，到達経路の特徴量から悪性サイトを高精度かつ迅速に検出する技術を研究開発しています（**図5**）．

今後に向けて

サイバーセキュリティリスクは，今や国家を脅かし得るものとなり，人類にとって極めて深刻な社会問題の1つといえます．攻撃側優位な状況が依然として続く中，私たちは本研究開発の推進によって，このサイバーセキュリティの厳しい現状を根本から打開し得る新たなセキュリティ技術を創出し，社会の発展に貢献していきます．

（上段左から）古賀　祐匠／中嶋　良彰／千葉　直子／三好　潤
（下段左から）小山　高明／司東　秀浩／宮島　麻美

私たちはサイバーセキュリティ対策やその運用にかかわるコストが企業のデジタルトランスフォーメーションを進めるうえでの妨げにならないような技術を創出することが，豊かな社会を創ることに資すると考え，この研究開発を推進しています．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
E-mail　scpflab＠hco.ntt.co.jp