Orchestrating a brighter world

NEC

資料4

NEC セキュリティ研究所のご紹介

2019年 1月

日本電気株式会社
セキュリティ研究所
所長　谷　幹也

中央研究所の組織と活動紹介

https://jpn.nec.com/rd/labs/index.html

約900名の研究者が活動

価値共創センター
中央研究所の技術を梃子に
NECの将来事業創造を加速

データサイエンス研究所
実世界の見える化と高度なデータ解析から人を超える予測・最適化、効率化を実現し、新たな社会価値を創造

バイオメトリクス研究所
認識・認証による人の理解を通じ
安全・安心・効率・公平を
誰もが手軽に享受できる社会を実現

2016/4 設立・約100名

セキュリティ研究所
社会インフラに対する様々な脅威から
システム・情報を守る
先進技術やソリューションを創出

システムプラットフォーム研究所
実世界に広く分布する処理基盤を
高効率かつ素早く柔軟に連携させる事で
AIによる社会価値創造の場を創出

北米研究所
- 複雑システム解析と管理技術
- 先端ネットワークとセンシング技術
- IoTシステムソリューション技術
- セキュリティ技術

欧州研究所
- ネットワークのソフトウェア化・仮想化
- 分散システム・セキュリティ
- IoTデータ並びにストリーミングデータのデータ分析
- IoTによるスマート・インフラストラクチャ・ソリューション

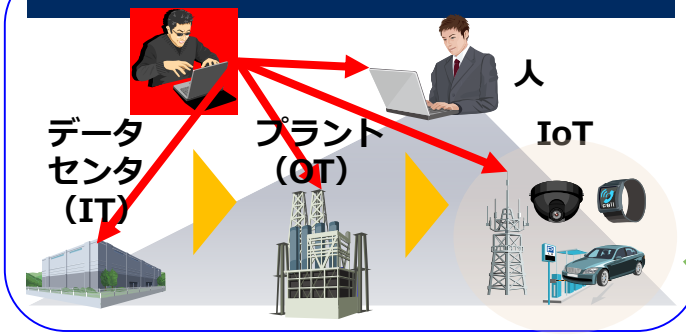
中国研究院
- 時空間データーアナリティクスと大気汚染への応用
- センシング技術と高齢者サービスへの応用
- 学習型最適化技術の研究と応用開拓
- 無線通信ネットワーク

シンガポール研究所
- 公共安全
- サイバーセキュリティ
- 公共交通
- 医療

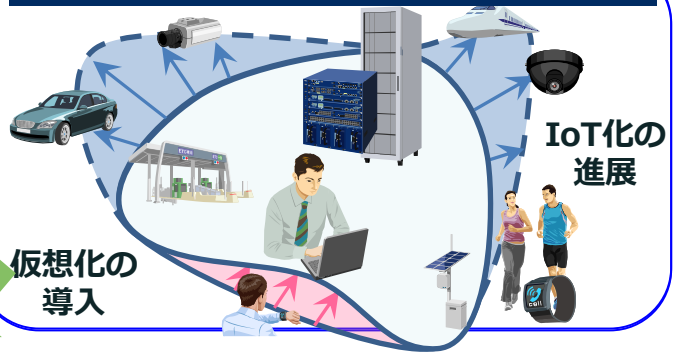
セキュリティを取り巻く環境と課題認識

守るシステムの範囲・複雑性・規模が拡大や、サイバー攻撃の高度化に対して、セキュリティ対策を根本的に見直す必要がある。

守るべき対象が大幅に拡大（サイバー・実世界[人含む]）



柔軟に変化するシステム



セキュリティ技術の革新が必要

高度化するサイバー攻撃

攻撃者の専門家集団

HWに仕込まれたマルウェア

実世界・サイバー連携攻撃

政府・業界の規制が強化

サイバーセキュリティ基本法

- サイバーセキュリティ戦略本部
- JC3（日本サイバー犯罪対策センター）
- 内閣サイバーセキュリティセンター
- J-CRAT（サイバーレスキュー隊）

セキュリティ研のミッション

セキュリティ研究所は、社会インフラの安定稼働を妨げる
様々な脅威からシステム・情報を守る先進技術やソリューションの
創出を通して、豊かで公平な社会の実現に貢献していきます。

社会システムの安全安心を提供

システムセキュリティ領域

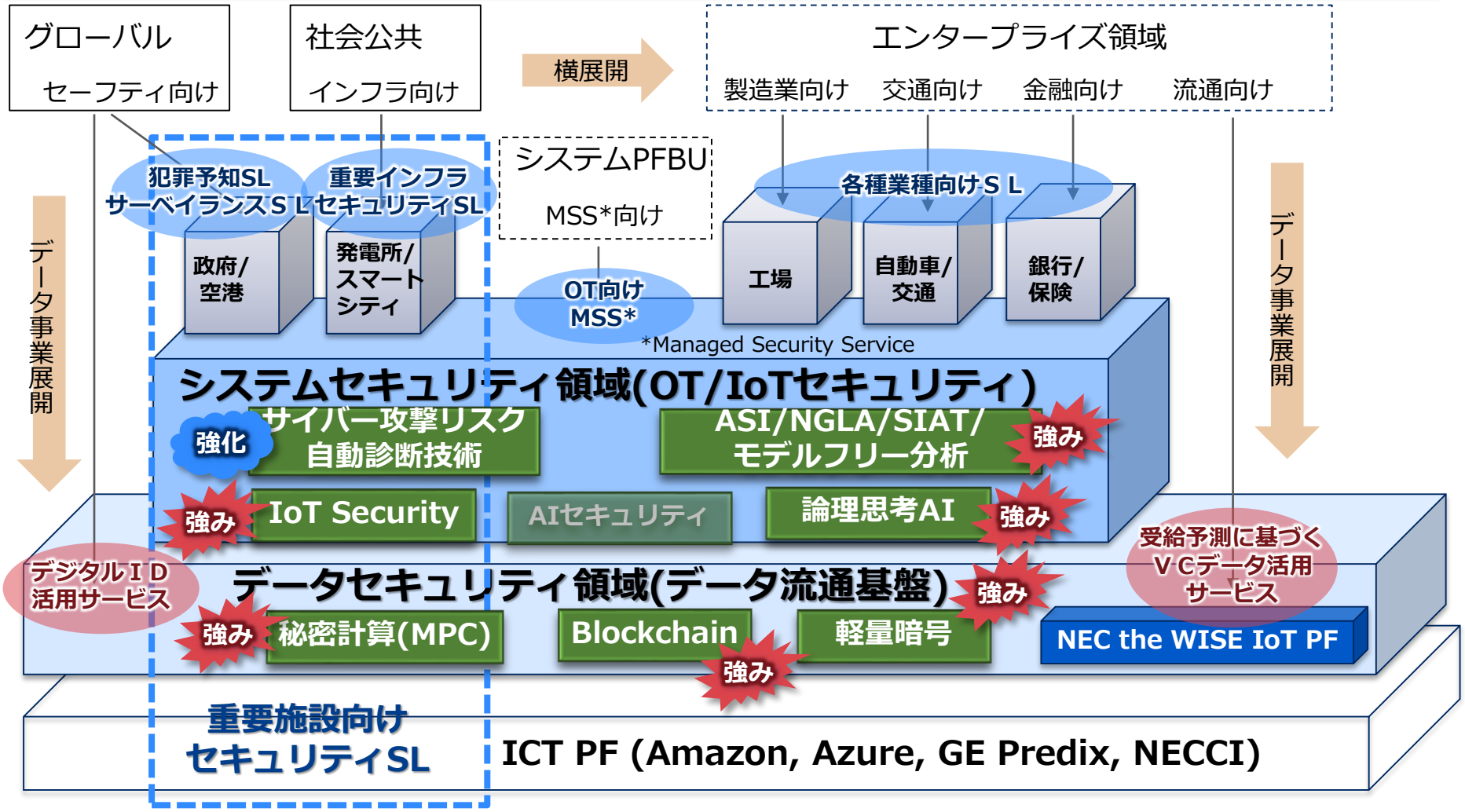
- OT/IoTセキュリティ
（仮想環境SEC診断・IoT機器セキュリティ）
- サイバー攻撃対策・予測
（インテリジェンス分析・AI分析）
- サイバー攻撃対策・異常検知
（要因分析技術）

データセキュリティ領域

- 高度暗号
（秘密計算・耐量子計算）
- 軽量暗号
（共通鍵/公開鍵/認証暗号）
- 分散台帳
（ブロックチェーン）

ビジネス展開を見据えたセキュリティ研究

重要施設向けセキュリティSL確立を当初目標としてPF構築を進め、データ共有PFの拡張によるデータ起点事業での他社先行を目指す



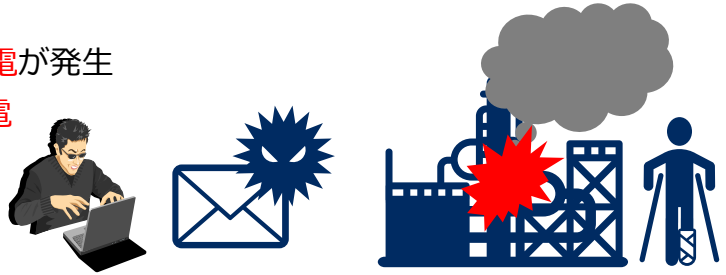
システムセキュリティ領域
(OT/IoTセキュリティ)

サイバー攻撃リスク自動診断技術（海外研究所連携）

2018/11/05広報<https://jpn.nec.com/rd/technologies/201804/index.html>

重要施設を狙う攻撃事例が増加

- 2008年　トルコの石油パイプラインで内部ネットワークに侵入。管内の圧力を異常に高めて爆発
- 2010年　イランのウラン濃縮施設で遠心分離機を破壊
- 2015年　ウクライナで変電所が攻撃され、3~6時間にわたる大規模な停電が発生
- 2016年　ウクライナで変電所が攻撃され、市内需要の5分の1が1時間停電



重要施設のセキュリティ診断の課題

- 組み合わせが膨大になり、網羅的な分析ができない
- 実システムを用いたテストができない

サイバー攻撃リスク自動診断技術とは？

- 実システムを仮想空間上にモデル化し、モデル上でセキュリティリスク診断を実施する技術

(現状)
人手で診断

工場・プラント
制御システム

機器構成

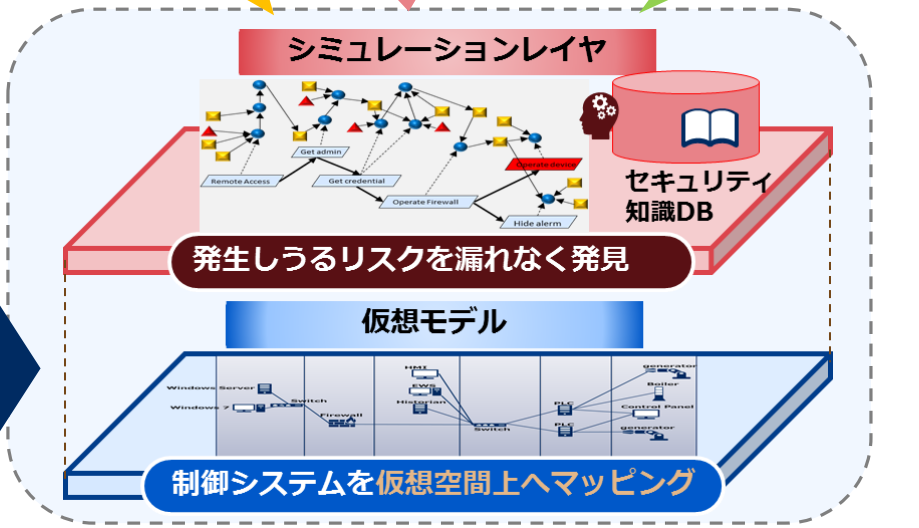
制御フロー

制御システムを仮想空間上へマッピング

いつでも
診断可能

網羅的に
分析

最新情報で
診断



サイバー攻撃対策技術（予測・対処の自動化）

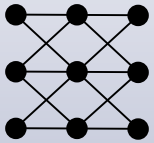
https://jpn.nec.com/cybersecurity/efforts/index.html

SNSやディープウェブからサイバー攻撃のトレンドを予測し、攻撃を受ける前に社会インフラを自動防御

攻撃者・犯罪者の発信～炎上

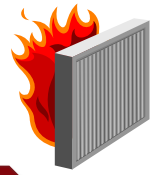
・攻撃者しか知り得ない悪性情報
・ハクティビストによる呼びかけ
・未公開の脆弱性や侵入手法

NEC Only1インテリジェンス分析アルゴリズム



Deep Neural Networkによる分析知識表現

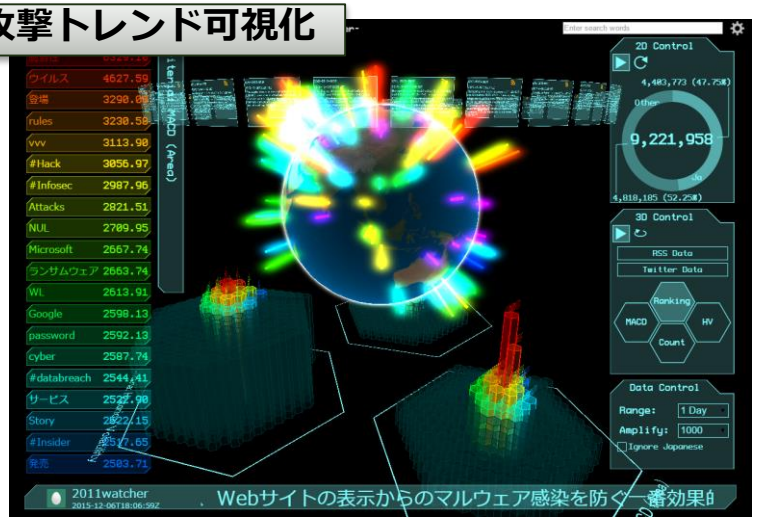
- アングラ観測
- トレンド分析
- クラスタ分析
- OSINT分析



社会インフラを守る現場

従来よりも48時間前に攻撃活動を検知して対処

攻撃トレンド可視化



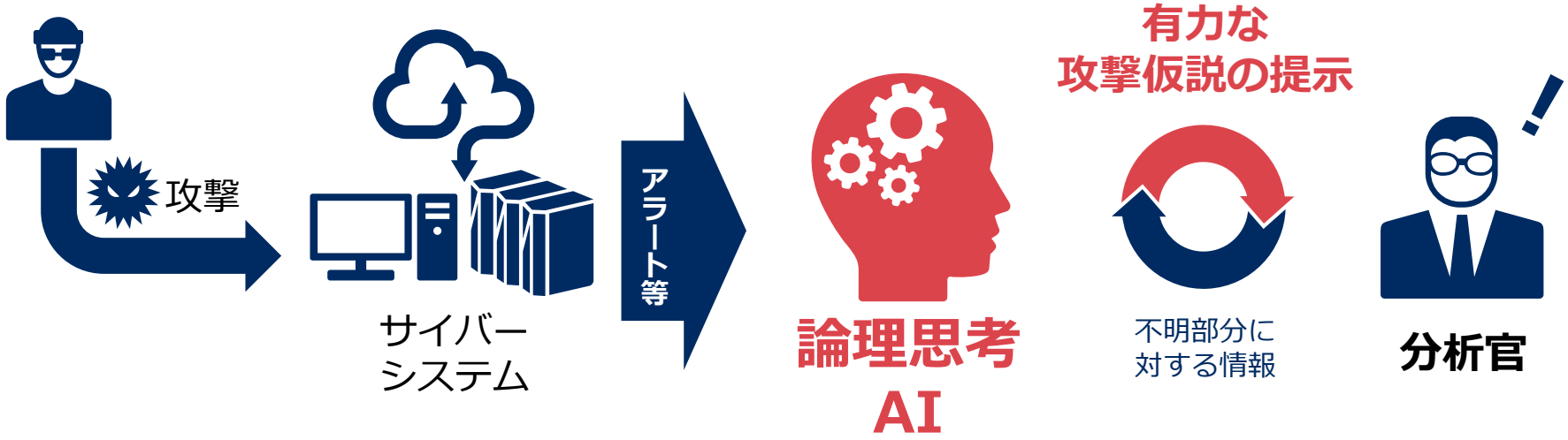
先進セキュリティオペレーション

AIによるサイバー攻撃の分析支援

根拠まで論理立てて説明できる論理思考AI (2018/12/12)
<https://jpn.nec.com/rd/technologies/201807/index.html>

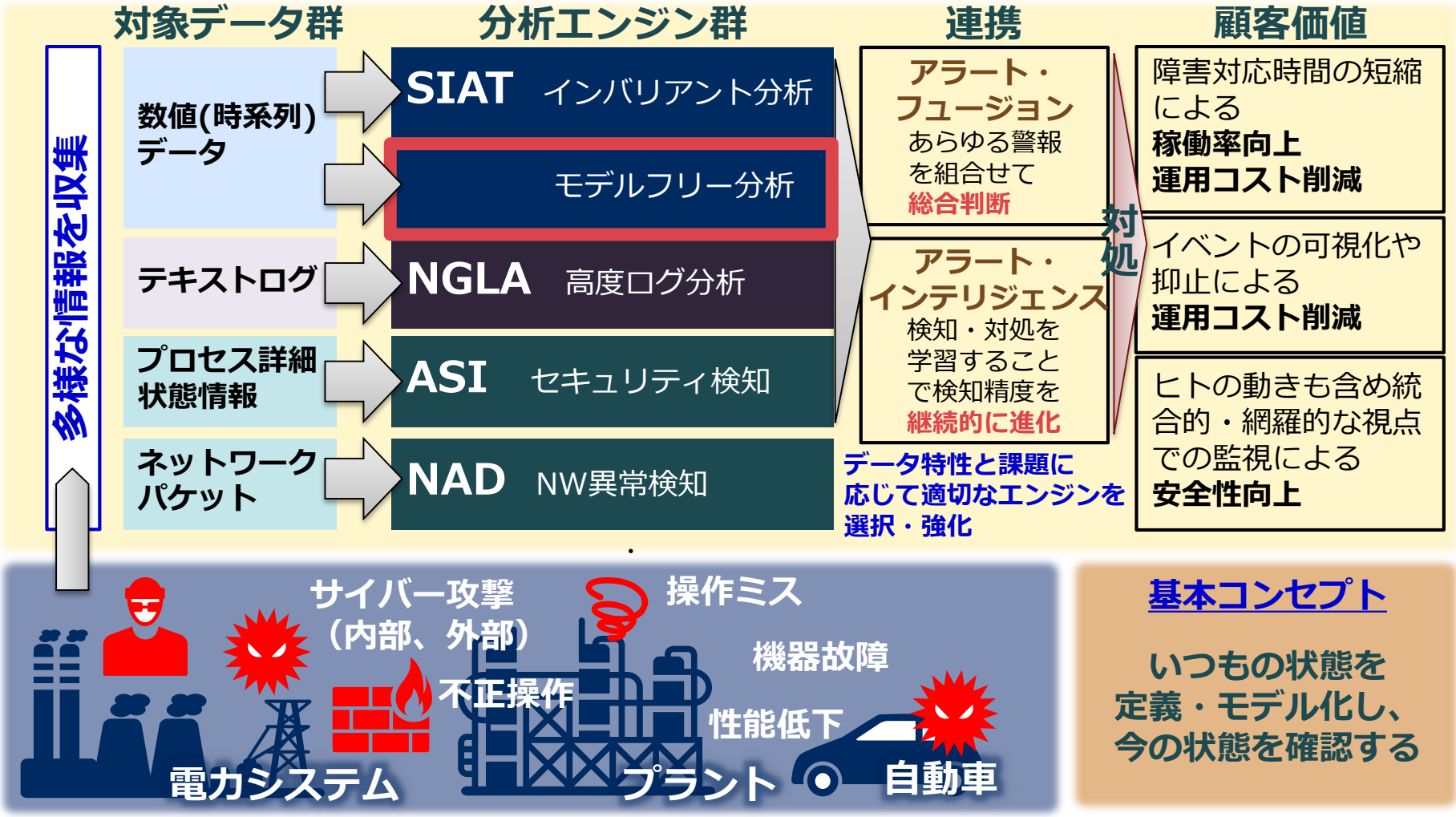
論理思考AIが、サイバー攻撃の手口の仮説等を提示しながら、
セキュリティ分析官と協働して高度な攻撃に対処

1. アラートや脅威情報を元に、
   ありうる脅威とその手口の仮説を生成
2. ログ、関連ファイル、脅威インテリジェンス等から
   証拠の候補を収集
3. 分析官との対話などにより**仮説を検証**



サイバー攻撃対策・異常検知/要因分析技術（北米研連携）

**データ特性に応じた分析エンジンの組み合わせにより、IT/OTシステムにおける
あらゆる異常を検知・原因特定し、迅速な対処を可能にするソリューションを確立**



基本コンセプト

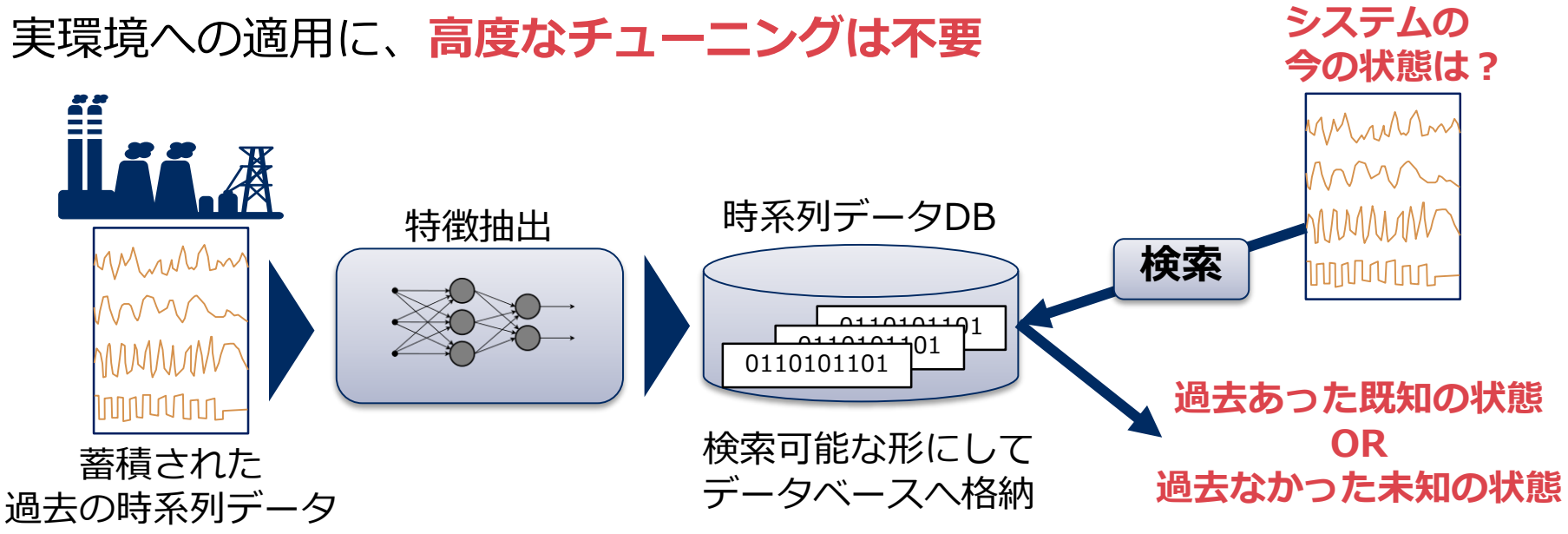
**いつもの状態を
定義・モデル化し、
今の状態を確認する**

モデルフリー分析：

2018/12/12広報<https://jpn.nec.com/rd/technologies/201806/index.html>

ドメイン知識によるチューニングなしに、
異常検知、障害診断、故障予測を高精度に実現する分析技術

- プラント等の時系列データを**モデル化（抽象化）せず**に、ディープラーニングを使って、**検索可能な形でデータベース化**
- システムの現在の時系列データを検索キーにして、データベースを検索することで、現在のシステムの状態が、過去にあった**既知の状態**か、過去になかった**未知の状態**か、を高精度、高速に判別
- 実環境への適用に、**高度なチューニングは不要**

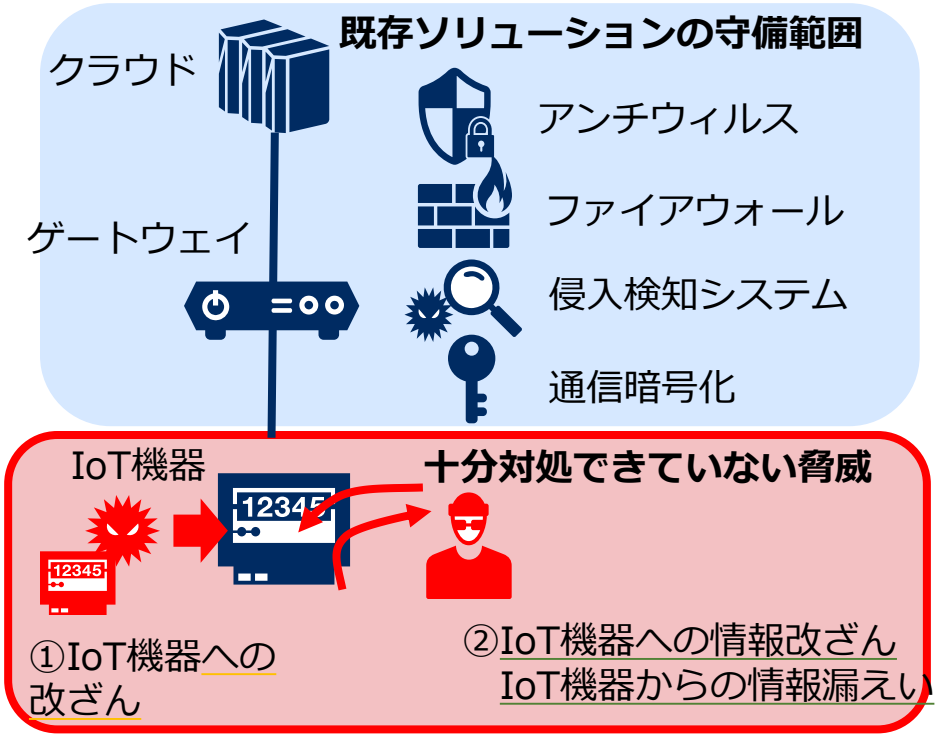


IoT機器セキュリティ

広報：IoTデバイス向け軽量改ざん検知技術(2018/04/02)
<https://jpn.nec.com/rd/technologies/falsification_find/index.html>

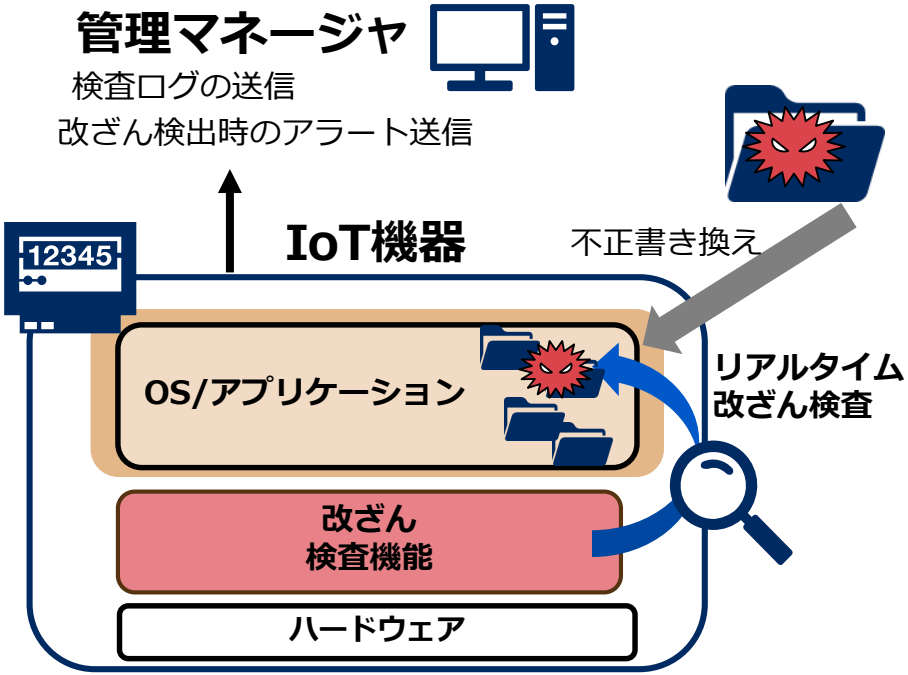
IoT機器のセキュリティ課題

- サーバやPCだけではなく、IoT機器も攻撃の対象となっているが、既存のソリューションで保護されていない

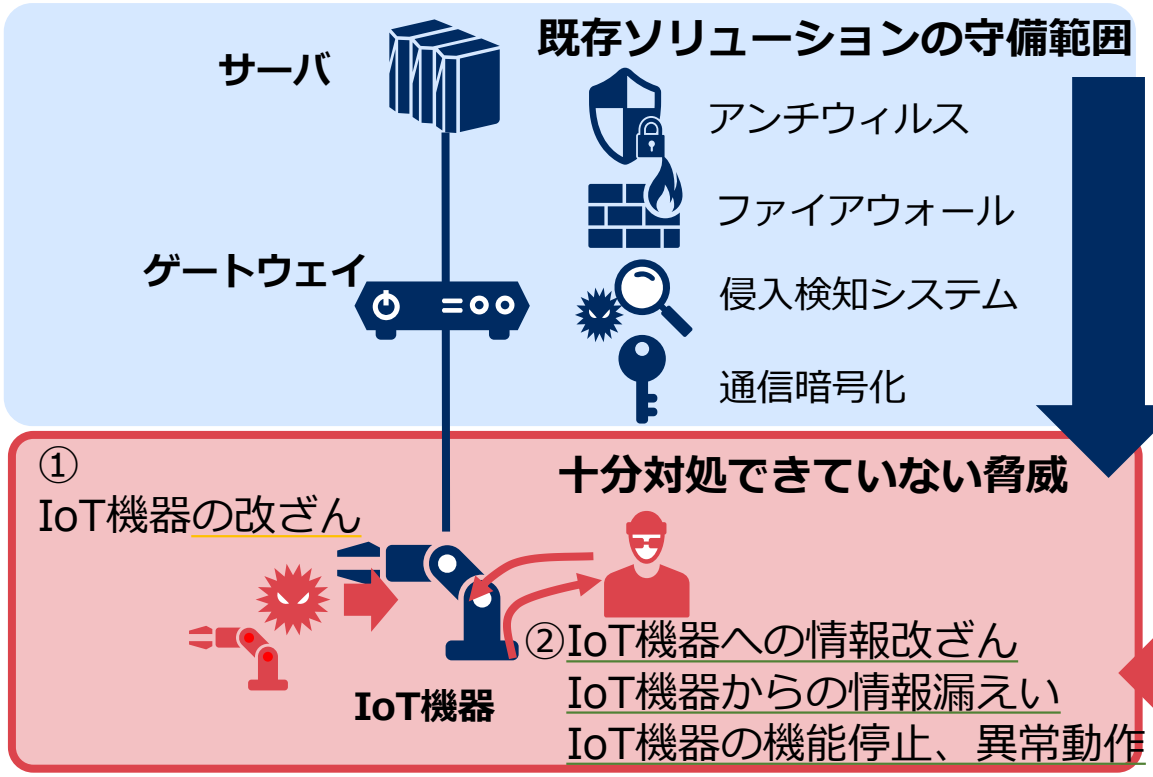


IoT機器の改ざんを高速に検知するソフトウェア検証技術

- IoT機器のソフトウェア改ざんを、機器の正常な状態(ホワイトリスト)を基に、改ざんをリアルタイムに検出



IoT機器に対するセキュリティ脅威



NWを介した攻撃：
IT系と同様、新種/
未知の攻撃は防げない

防御を通過した新種攻撃
NWを介さない直接攻撃

従来型の対策だけでは不十分な懸念が大きく、
IoT機器自体へのセキュリティ保護機能の導入が望まれる

IoT/OT機器に対するサイバー攻撃事例

IoT/OTを狙う攻撃被害が、すでに現実の脅威となっている

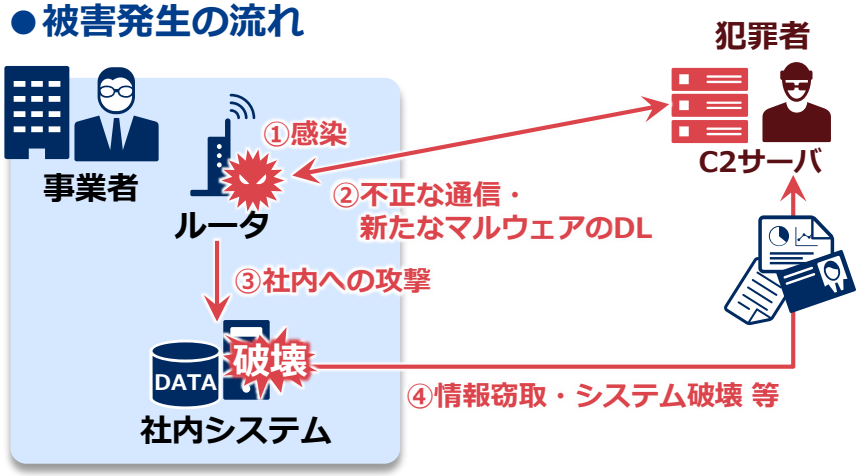
IoTへの攻撃 (マルウェア：VPNfilter)

2018年5月

攻撃対象	小規模事業者・個人向けルータ
攻撃目的	情報窃取・システム破壊 等
被害規模	54か国・50万台以上

※Trendmicor社報告による　https://blog.trendmicro.co.jp/archives/17484

●被害発生の流れ



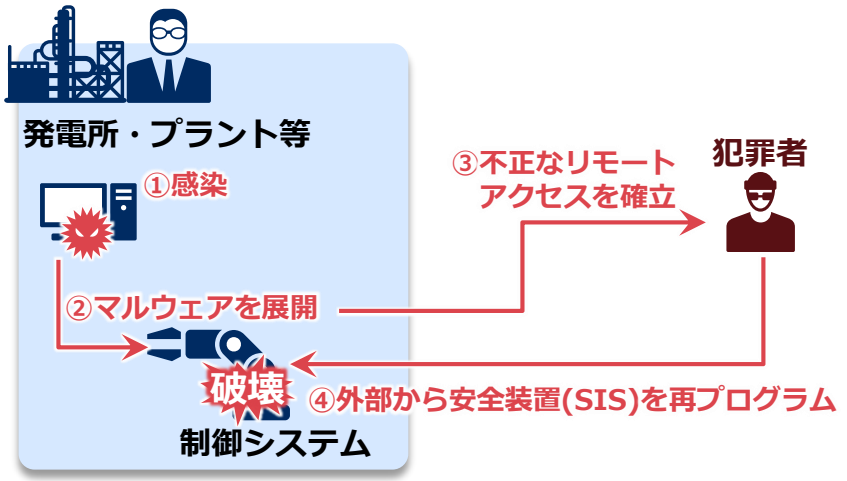
OTへの攻撃 (マルウェア：TRITON)

2017年12月

攻撃対象	制御システムの安全装置(SIS)
攻撃目的	安全装置の不正操作による 制御システムの破壊 等
被害事例	中東で工場の操業が一時停止

※fireeye社報告による　https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

●被害発生の流れ

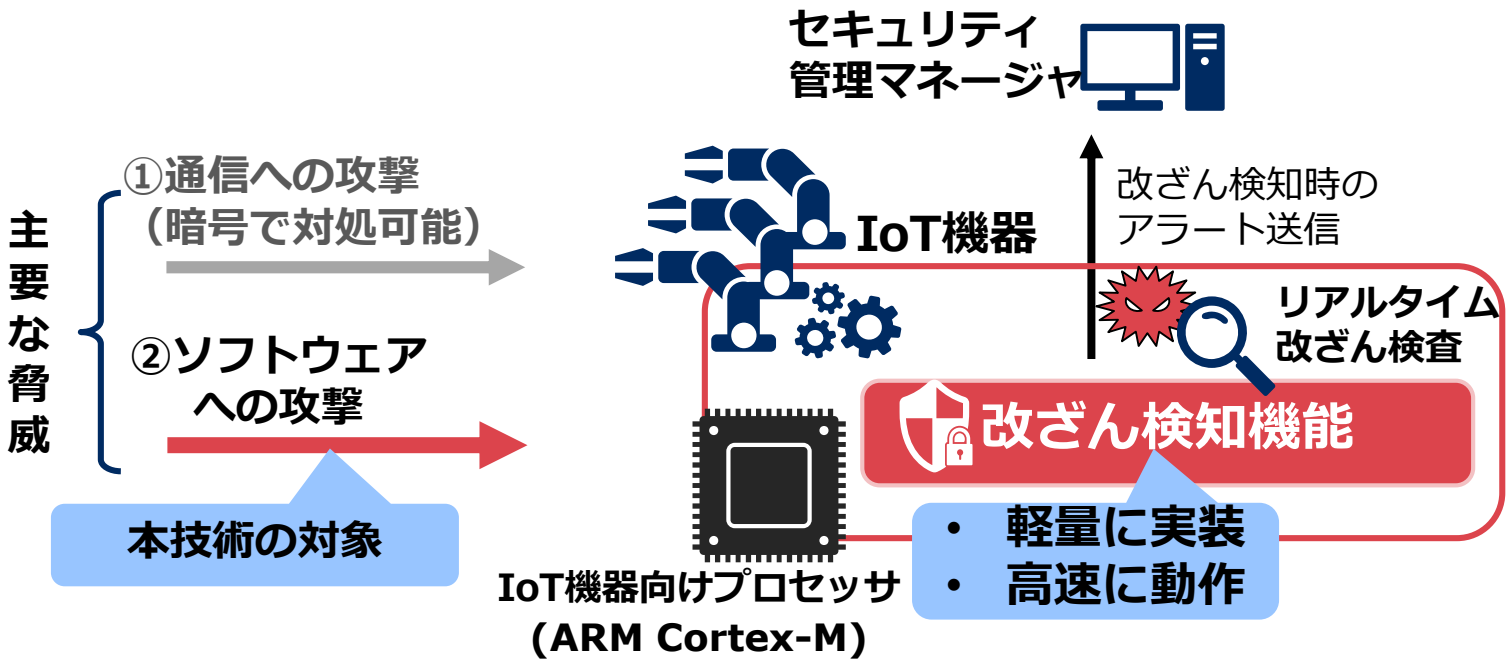


IoT機器向けソフトウェア改ざん検知：概要

IoT機器のソフトウェア改ざんを、機器の正常な状態(ホワイトリスト)を基に、リアルタイムに検知

NEC技術の特徴

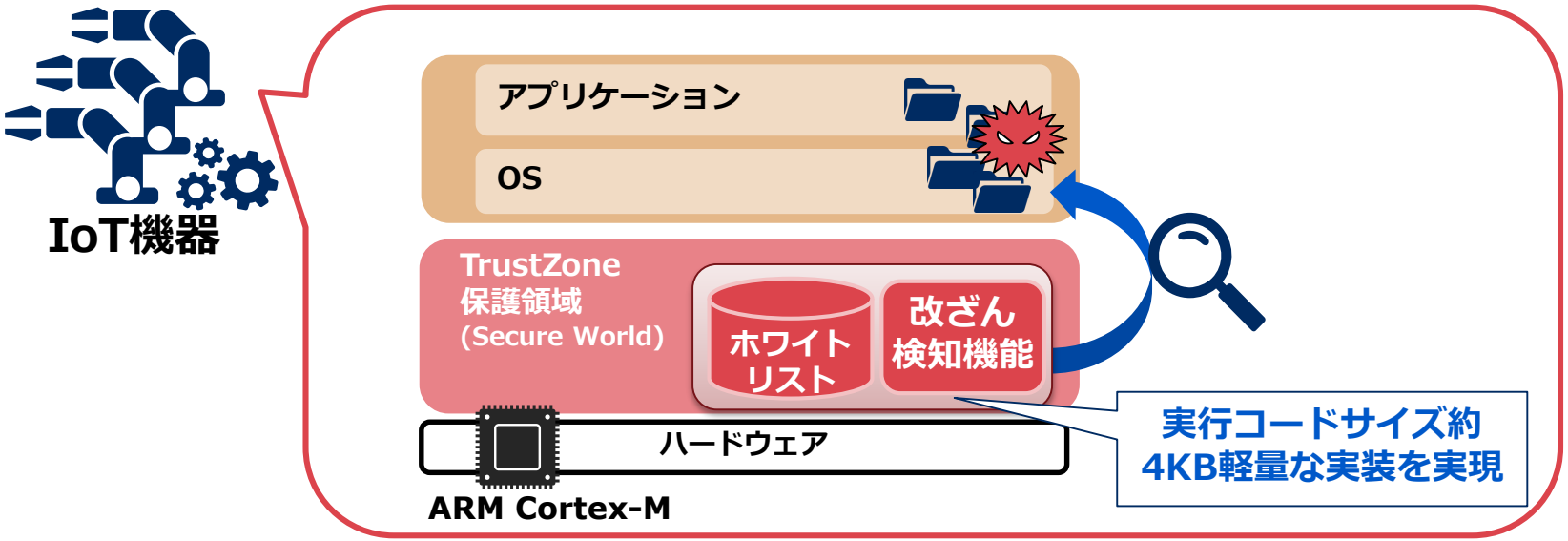
- **軽量性**：メモリ容量が小さいIoT機器にも適用可能な軽量実装
- **高速性**：検査領域を限定することで、高速な改ざん検知を実現



NEC技術の特徴：軽量性

改ざん検知を約4KBの実行コードで軽量実装できるアーキテクチャを開発

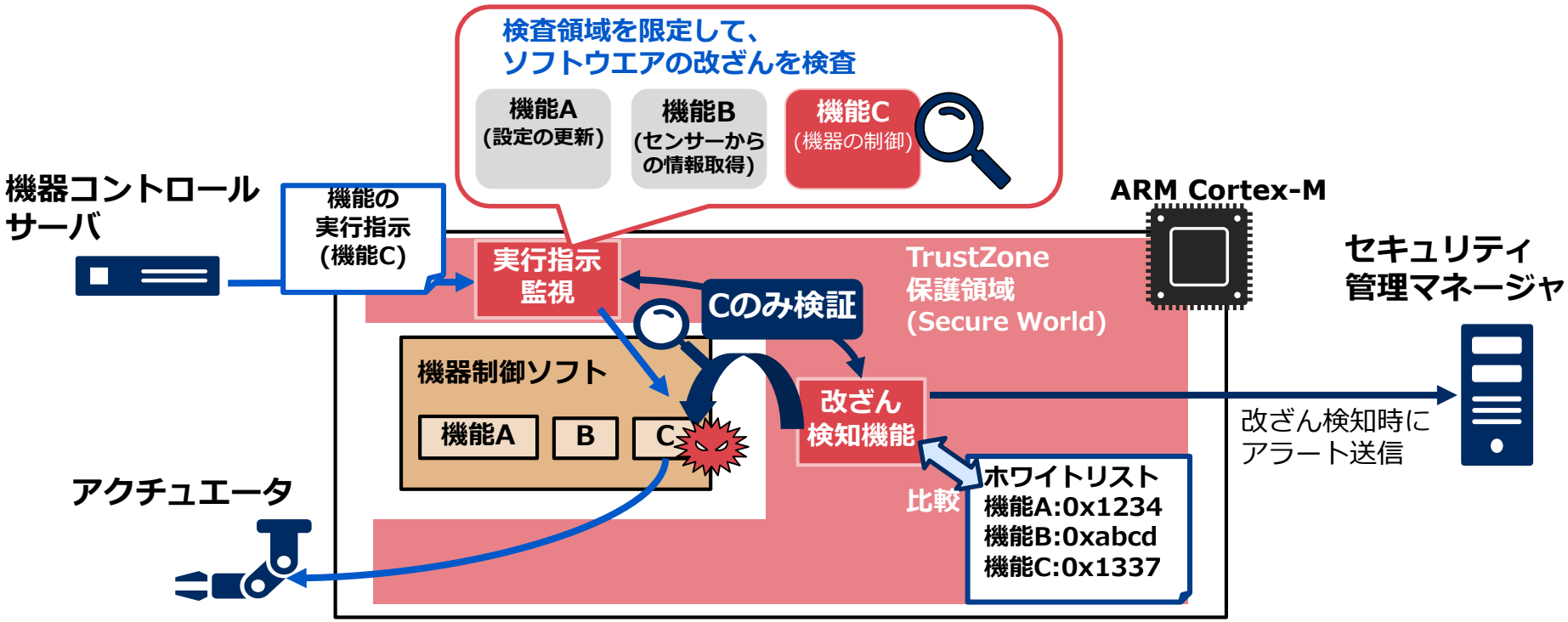
- メモリ上に保護領域を構築する機能(ARM TrustZone)を用いて、改ざん検知機能を実装
  - これにより、本機能自体を保護するための実行コードを追加することなく、改ざん検知機能自体への攻撃や無効化を防止
- ソフトウェアの制御等による機器の複雑なふるまいを監視するのではなく、実行コードのみ監視を行うシンプルな方式を採用
- **メモリ容量が少ないセンサーなどにも適用が可能**



NEC技術の特徴：高速性

検査領域を絞り、2KBの機能を約６ミリ秒で検査可能な高速な改ざん検知技術を開発

- OSやアプリケーションなどのソフトウェアの構造を機能ごとに把握し、機能の実行処理の指示を基に、これから実行されるコードが格納されているメモリ領域を特定
- その領域に絞って改ざんの有無を検査することで高速化
- **搬送ロボットなどの遅延が許容されない機器にも適用可能**



軽量改ざん検知による攻撃への対応

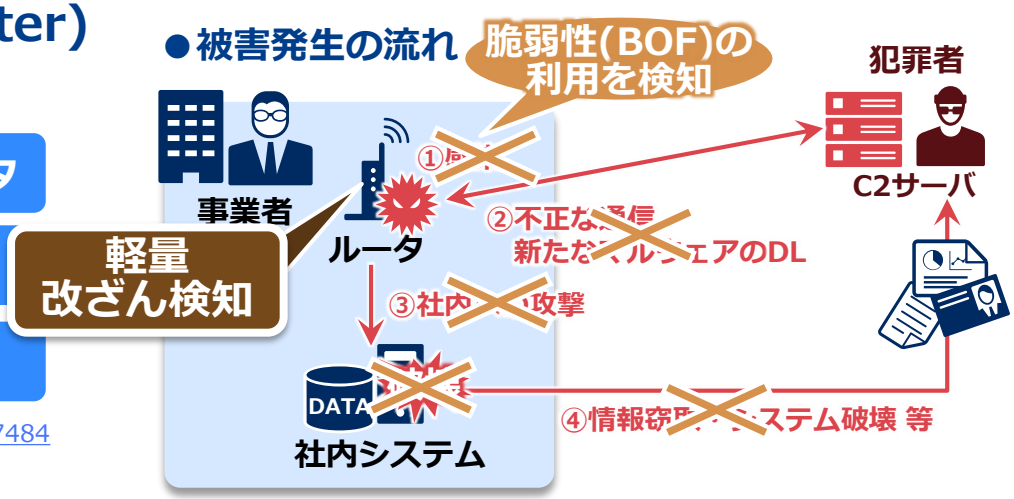
IoT/OTへの攻撃を軽量改ざん検知により検出することが可能

IoTへの攻撃 (マルウェア：VPNfilter)

2018年5月

攻撃対象	小規模事業者・個人向けルータ
攻撃目的	情報窃取・システム破壊 等
被害規模	54か国・50万台以上

※Trendmicor社報告による https://blog.trendmicro.co.jp/archives/17484

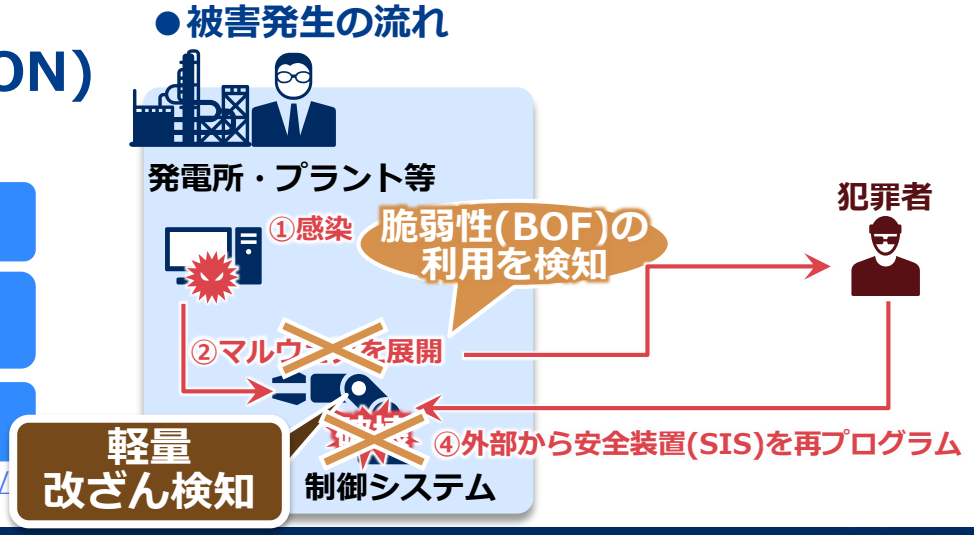


OTへの攻撃 (マルウェア：TRITON)

2017年12月

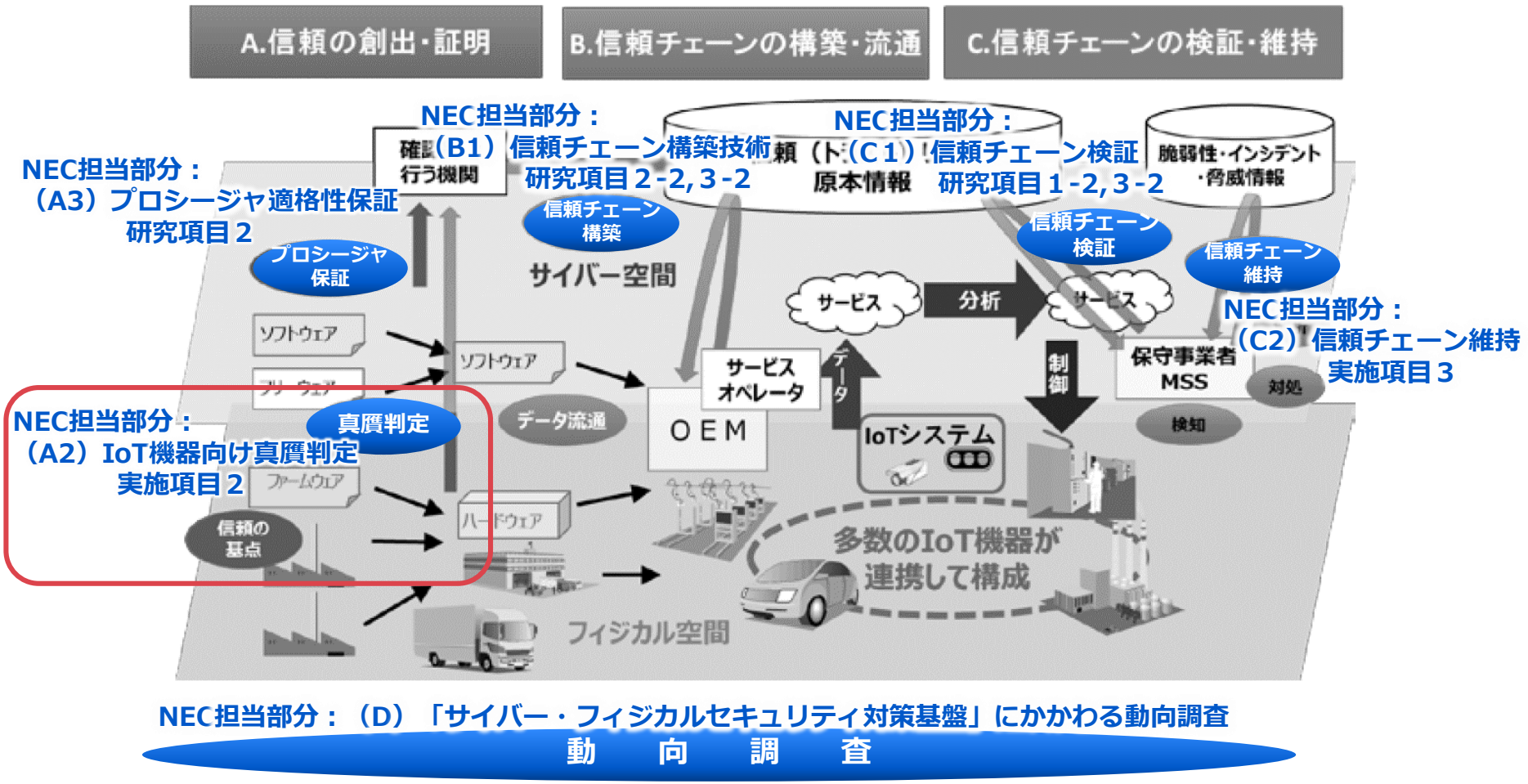
攻撃対象	制御システムの安全装置(SIS)
攻撃目的	安全装置の不正操作による制御システムの破壊 等
被害事例	中東で工場の操業が一時停止

※fireeye社報告による https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html



SIP(第2期)（サイバーセキュリティ）概要

IoT機器セキュリティ
(補足)



図表２－１．　信頼チェーンで構築されるサイバー・フィジカル・セキュリティ対策基盤のイメージ

出典：平成３０年７月１９日　戦略的イノベーション創造プログラム（SIP）IoT社会に対応したサイバー・フィジカル・セキュリティ研究開発計画

データセキュリティ領域
(データ流通基盤)

データ流通基盤

データ流通サービスの社会実装を、信頼性とプライバシー保護を両立するセキュアなデータ流通基盤技術(暗号/BlockChain/秘密計算)により実現。

安心してデータ交換可能なデータ流通基盤

- No.1コア技術(MPC,BC,軽量暗号)を基にデータ信頼性とプライバシー保護を実現するセキュアなデータ共有を実現

社会実装・政策提案と連携する新しい研究開発

- 研究開発と並行して社会実装・レギュレーションへの反映を目指す。

「データ流通基盤」

BlockChain No.1 処理性能1000倍(従来比)で最難関国際学会10件以上採択

複数組織でデータの信頼性を担保

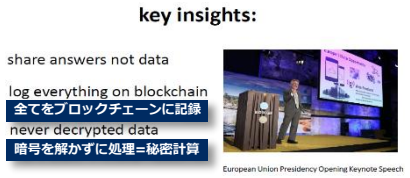
秘密計算技術 No.1 処理速度200倍(従来比)で最難関国際学会3件に採択

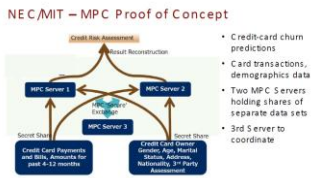
複数組織の機密データを相互開示せずに結合

NECの強いNo.1技術を基盤に実装することで処理結果だけを安全に流通

社会実装への取り組み

- mit media lab MITデータ共有コンソーシアム
- JPX SBI JPXでのKYC実証実験
- WORLD ECONOMIC FORUM 第4次産業革命センター





レギュレーションへの提案

- 国際間での制度改正で省庁へ働きかけ

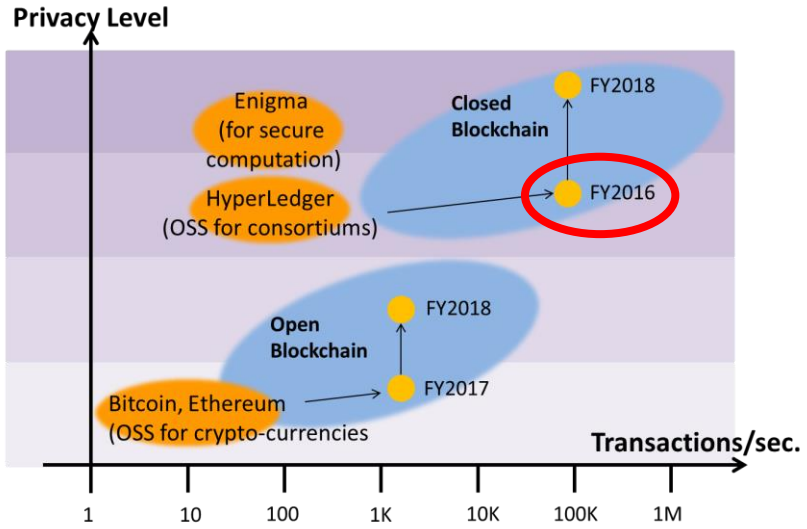
ブロックチェーン技術(欧州研連携)

2018年2月15日広報<https://jpn.nec.com/press/201802/20180215_03.html>

既にNECには強いブロックチェーン技術がある。他社比千倍高速な処理と、データ開示範囲を制御する機能を実現済み。

世界No.1の技術を実現、特許15件、研究論文10件

- ビットコイン創生期から
  ブロックチェーンセキュリティを研究
- **世界最高速の処理性能**
  10万トランザクション/秒を実現
- 取引の透明性と秘匿性を両立する
  独自のデータ開示制御を実現



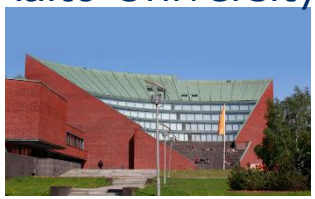
社外技術との比較とロードマップ

アカデミアおよびOSSコミュニティとの強いパイプ

アカデミアとの
セキュリティ研究

ETH Zurich

Aalto University



オープンソースプロジェクトに
Premier Memberとして参画 (2017年6月)

HYPERLEDGER

安全なデータ活用を実現する秘密計算

2018年11月5日広報<https://jpn.nec.com/rd/technologies/201805/index.html>

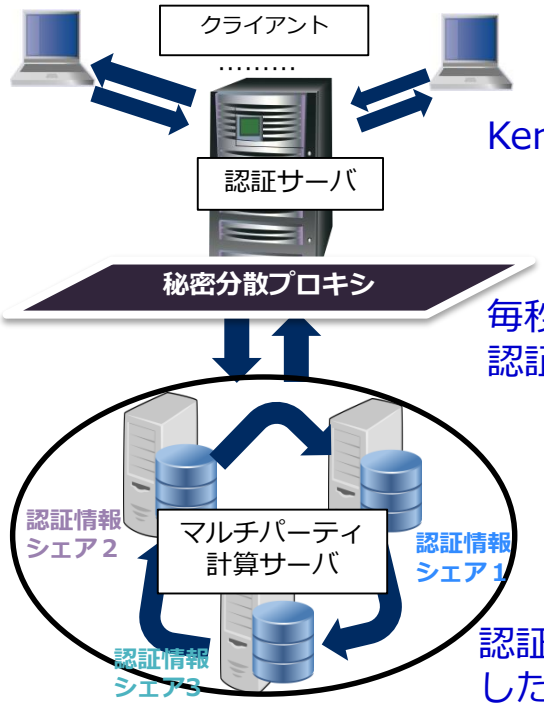
データを複数サーバに秘密分散し、秘匿したまま処理するマルチパーティ計算技術で世界トップレベルの技術を創出

国際的に高い評価を得て、難関国際学会に採択。
CCS2016(Best Paper)**、Eurocrypt2017、S&P2017、CCS2018**

- データの処理中も含め、情報を一切漏らさない強固なデータ漏えい防止を実現
- 基本アルゴリズムの改良に成功し、飛躍的な性能向上に成功。従来方式と比較して14倍の高速処理を達成

マルチパーティ計算の最近の進歩

提案年度	方式	スループット [AES処理件数 / 秒]
2013	他社方式	約3,500
2016	他社方式	約25,000
2016	他社方式	約90,000
2016	**NEC方式**	**約1,300,000**



軽量暗号技術（認証暗号）

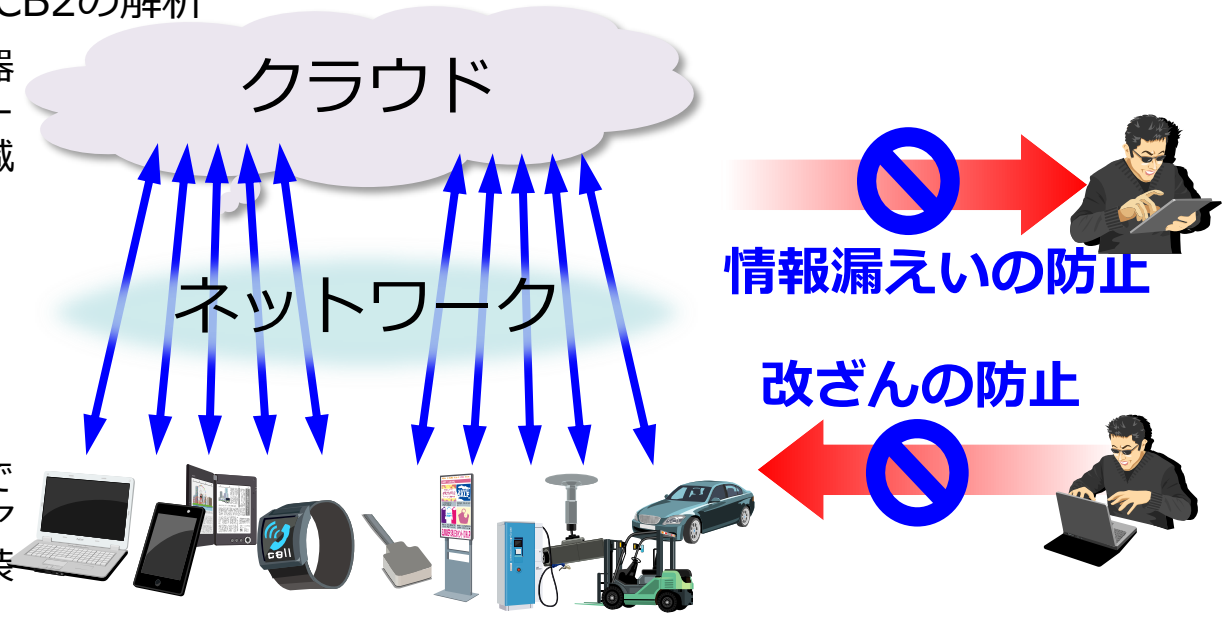
2015年7月21日広報<https://jpn.nec.com/press/201507/20150721_04.html>

- IoTの利用拡大にともない、データの秘匿と改ざん検知を安全かつ効率的に実現する認証暗号技術が重要に
- 認証暗号に関する最先端の研究を推進
  - 暗号化と同じ計算量で、暗号化と改ざん防止を同時に実現する、認証暗号技術OTR（Eurocrypt 2014)
  - 初期ベクトル不要な認証暗号ZMAC/ZAE (CRYPTO 2017)
  - LINEの暗号化方式の解析（ESORICS 2018)
  - 国際標準の認証暗号方式OCB2の解析

NECの認証暗号技術の効果

高速暗号処理
膨大な数の機器と通信するサーバの負担を軽減

暗号適用可能なデバイスの拡大
ハードウェアでもソフトウェアでも小さな実装




Orchestrating a brighter world
NEC