IoT向けサイバー攻撃検知技術とSOCによる監視サービス

Cyber Attack Detection Technology for IoT and Monitoring Service by SOC

芳賀 智之 Tomoyuki Haga
大庭 達海 Tatsumi Oba
田崎 元 Hajime Tasaki
鴨川 郷 Akira Kamogawa
佐々木 崇光 Takamitsu Sasaki
松島 秀樹 Hideki Matsushima

要　旨

自動車，ホーム，工場，ビルなどフィジカル空間とサイバー空間の融合されたCPS（Cyber Physical System）においては，サイバー攻撃がフィジカル空間へ波及し，人命リスクにつながるため，サイバー攻撃への対策が不可欠となる．特にIoT機器は，ITと異なり独自の通信が多いため，独自の対応が必要になる．そこで当社では，AIによる異常検知技術を応用し，IoT機器の制御コマンドやネットワークに着目したサイバー攻撃攻撃検知技術と，効率的な分析を可能にするキルチェーン分析技術を用いたIoT向けSIEM（Security Information and Event Management)を開発している．さらに制御システムの監視における課題と，制御システムの一例として工場SOC（Security Operation Center）サービスで実施される対策と運用について述べる．

Abstract

In a Cyber Physical System (CPS) such as automobiles, homes, factories, and buildings where the physical space and cyber space are integrated, cyber-attacks spread to the physical space and lead to a risk to human life. Therefore, countermeasures against cyber-attacks are indispensable. In particular, IoT devices are different from IT communication in terms of their unique communication protocols; hence, specific measures are needed for them. Therefore, we use AI-based attack detection technology that specializes in cyber-attacks by focusing on control commands and networks of IoT devices. We are developing IoT-SIEM (Security Information and Event Management) using kill chain analysis technology that enables efficient analysis. Furthermore, we describe the issues in monitoring the control system and the measures and operations of Factory SOC (Security Operation Center) service as an example of the control system.

1. はじめに

IoT化に伴い，自動車，ホーム，工場，ビルなどフィジカル空間とサイバー空間の融合されたCPS（Cyber Physical System）においては，サイバー攻撃がフィジカル空間へ波及し，人命リスクにつながるため，サイバー攻撃へのリスクが高まっている．特に，IoTデバイスは，ITとは異なり，独自の通信を用いている．例えば，自動車ではCAN (Controller Area Network)，ビルではBACnet™といった独自の通信を利用している．

自動車においては，2015年に遠隔から車両CANを介して不正制御できることが実証され，セキュリティ対策目的としては初のリコールへと発展した[1]．ビルシステムでは，2016年にはフィンランドにあるビルがDDoS攻撃を受けて暖房システムが機能停止し，工場ではWannaCryによるサイバー攻撃で操業停止となる事例が多く発生している．こうしたなか，各分野で法制化やガイドラインが策定されている．自動車向けでは，国連の自動車基準調和世界フォーラム（WP29）による自動車サイバーセキュリティ対策の国際基準[2]が成立し，各国で法制化が進んでいる．また，ビルやスマートホームシステム向けには，経済産業省がサイバー・フィジカル・セキュリティ対策ガイドライン[3][4]を策定している．

このような法規制やガイドラインに対応していくために重要とされるのは，侵入後の被害を最小限に抑えるための「検知」「対応」「復旧」である．これらのセキュリティライフサイクルを実現するために，攻撃を早期に検知するためのSIEM（Security Information and Event Management）が必要であり， SIEMを使った監視組織であるSOC（Security Operation Center）が重要となる．

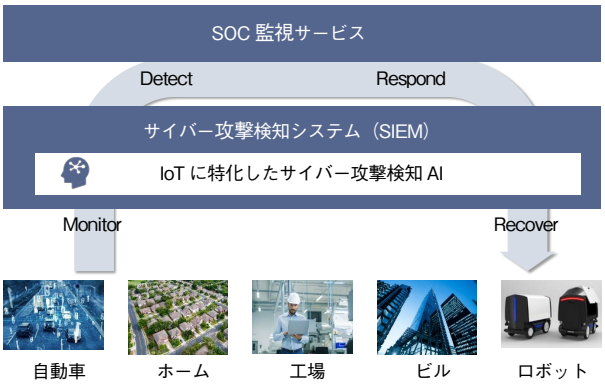
2. 当社のIoTサイバーセキュリティシステム

当社では，人工知能（AI）を使ったIoT向けサイバー攻撃検知システムの開発に取り組んでいる．

IoT機器側にはルールベースの攻撃検知エンジンを，クラウド側にはAIを使った攻撃検知エンジンを配置し，多層の検知エンジンでIoT機器のセキュリティ状態を監視する．

AIを使った攻撃検知エンジンは，正常時のIoT通信ネットワークデータを学習して正常状態をモデル化し，そのモデルと逸脱したデータを異常として捉える機械学習ベースの異常検知手法である．

IoTサイバーセキュリティシステムでは，**第1図**に示すように，まずIoT機器から大量のログを監視・収取（Monitor）し，IoT-SIEM（以降はSIEMと記述する）を用いて脅威の可視化・検知（Detect）を行う．そこで重大なインシデントを検出した場合には，SOCのセキュリティ分析官は，SIEMを使って攻撃分析を行い，インシデント対応部隊のSIRT（Security Incident Response Team）と連携し，対応（Respond）する．その後，攻撃検知エンジンを新しい攻撃に対応できるよう更新して復旧（Recover）する．

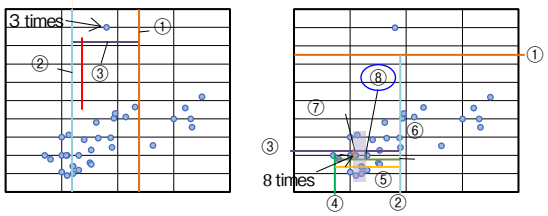


第1図　IoTサイバーセキュリティシステム
Fig. 1　IoT cybersecurity system

3. AIを用いたサイバー攻撃検知技術

3.1 制御コマンドに対する異常検知手法

本節では，制御システムにおける制御コマンドやセンサ値のAIを用いた異常検知技術について説明する．代表的な異常検知手法としてLOF（Local Outlier Factor）があるが，自動車等の制御システムネットワークのメッセージの評価の際に，大量のデータを保持しなければならず，さらに計算量も多い．そこで，メモリー量と計算量が小さいIsolation Forestを用いる異常検知アルゴリズムに着目した．

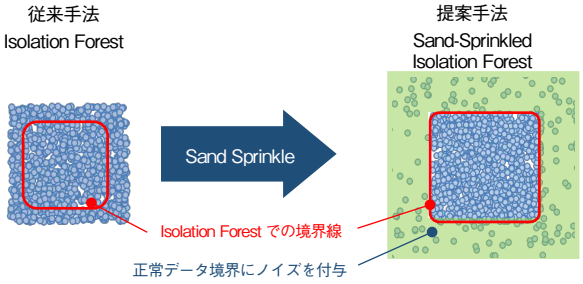


(a) 疎な部分のデータ　(b) 密な部分のデータ

第2図　Isolation forestの概要
Fig. 2　Abstract of an isolation forest

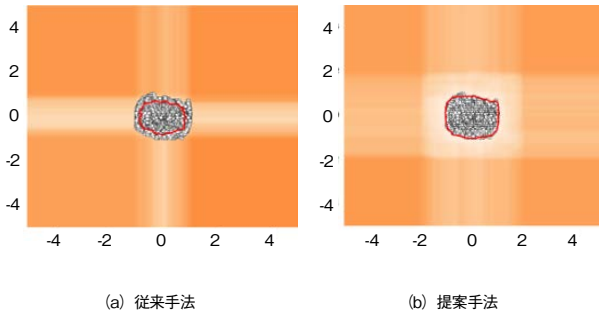
Isolation Forestは，正常・異常のラベルがついていない訓練データを入力とし，訓練データの疎密に基づいて正常データと異常データを分類するアルゴリズムである．データの疎密は，訓練データが1点になるまでの分割数で判断される．疎な部分の点の分割数は**第2図（a）**のように比較的小さく，**第2図（b）**のような密な部分点の分割数は大きくなる．Isolation Forestでは，分割数で異常度を判断する手法で，分割数が小さいほど異常度が高いと判断される．

しかし，単純にIsolation Forestを使い，自動車の通常走行時のCANデータで学習を行うと，**第3図**のように正常と異常の識別境界が正常データの境界よりも内側に引かれ，誤検知が増加してしまうという課題がある．これは外側の正常データが疎となるために発生する課題である．



第3図　Sand sprinkled isolation forest
Fig. 3　Sand sprinkled isolation forest

正常・異常が混在しているデータではなく，正常なデータのみを保持している場合，訓練データに対する検知が少なくなるような識別境界を得たい．この目的を達成するために，訓練データに**第3図**のような一様ノイズを加えたうえで学習を行うSand Sprinkled Isolation Forestを提案している[5].



(a) 従来手法　(b) 提案手法

第4図　従来手法と提案手法の識別境界
Fig. 4　Isolation forest and sand sprinkled isolation forest

正規化した実車のCANデータに対して，正常なデータのみで従来手法のIsolation Forestと提案手法のSand Sprinkled

Isolation Forestで識別境界を引いた場合の結果を**第4図**に示す．従来手法であるIsolation Forestの識別境界は，正常データの内側に引かれている．一方，提案手法では，ノイズの疎密を調整することで，訓練データの疎な部分を内側に含むような識別境界を得ることができた．

実際に攻撃を含まない正常データと，攻撃を含むデータを対象に評価を行った結果を**第1表**に示す．提案手法では，従来手法に対してTrue Positive Rate（TPR）を維持しつつ，False Positive Rate（FPR）を大きく低減させることが確認できた．

第1表　実車CANデータに対する評価結果
Table 1　Result of the CAN data of a real vehicle

		従来手法 [%]	提案手法[%]
攻撃含まないCANデータ	TPR	-	-
	FPR	28.85	0.16
攻撃含むCANデータ	TPR	99.75	99.67
	FPR	0.149	0.008

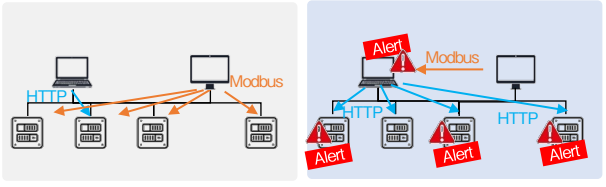
3.2.　制御ネットワークに対する異常検知手法

本節では制御システムネットワーク内で発生する通信のサーバ側，クライアント側のIPアドレス，TCP/UDPのポート番号の組み合わせ（以降通信トリプレット）（**第2表**）を用いた異常検知手法（GCN SCOPE）[6]を紹介する．

第2表　通信トリプレットの例
Table 2　Examples of communication triplets

s (server's IP address)	*p* (TCP/UDP port number)	*c* (client's IP address)
192.168.1.10	UDP/2222	192.168.1.30
192.168.1.20	UDP/137	192.168.1.10
192.168.1.20	TCP/139	192.168.1.40
…	…	…

制御システムは，その性質上**第5図**に示す通信トリプレットのホワイトリストを用いた異常な通信の検知手法が有効だと考えられている[7][8]が，学習不足さや非定常的な操作（メンテナンス，トラブル対応など）のために発生する通信の影響により誤検知を大量に発生させてしまうケースがある．

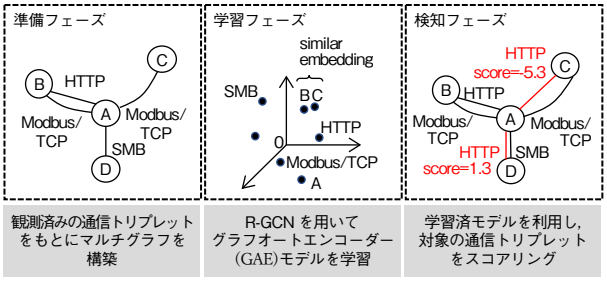


第5図　通信トリプレットのホワイトリストベース検知方式
Fig. 5　Whitelisting method using communication triplets

そこでGCN SCOPEでは，ホワイトリストに存在しない通信トリプレットに対する異常度の算出を行い，その異常度が閾（しきい）値を上回っている場合にのみアラートを発生させ誤検知を回避することを考える．

これは観測済みの正常な通信トリプレットに基づいて，未観測の通信トリプレットの存在性を予測するリンク予測問題に帰着される．

リンク予測にはマルチグラフに適用できるグラフ畳み込みニューラルネットワーク（R-GCN）[11]を活用することができる．あらかじめ観測された通信トリプレットを元に通信マルチグラフ（ノードが各デバイス，エッジの種類はサーバ側のTCP/UDPポート番号）を構築しておき，R-GCNモデルを学習することでノードとエッジのベクトル表現を得ることができる．このベクトル表現を用いて任意の通信トリプレットに対して異常度を算出することができる．GCN SCOPEの全体的な処理の流れは**第6図**のとおりである．



第6図　GCN SCOPEによるリンク予測の流れ
Fig. 6　Link prediction flow of a GCN SCOPE

当社の3つの工場で，それぞれ1週間の通信データを収集・学習し，その後1週間の間に実際に現れた通信トリプレットとランダムに混入した通信トリプレットを識別させるタスクを実行した際のROC AUCの値を**第3表**に示す．実験では，ベースラインとしては2つのヒューリスティックな比較手法1と比較手法2を利用した．それぞれfirst-order proximityとsecond-order proximityに基づくリンク予測手法[12]である．GCN SCOPEはこれら2つの比較手法を圧倒するAUCを示しており，アラート監視の効率化に寄与できると考えられる．

第3表　ICSの実データに対する正常/異常判別時のROC AUC
Table 3　ROC AUC of link distinction on real ICS datasets

異常度算出手法	Factory A	Factory B	Factory C
GCN SCOPE（提案手法）	**0.962**	**0.914**	**0.996**
比較手法1	0.853	0.735	0.771
比較手法2	0.820	0.632	0.769
ランダム異常度	0.512	0.521	0.519

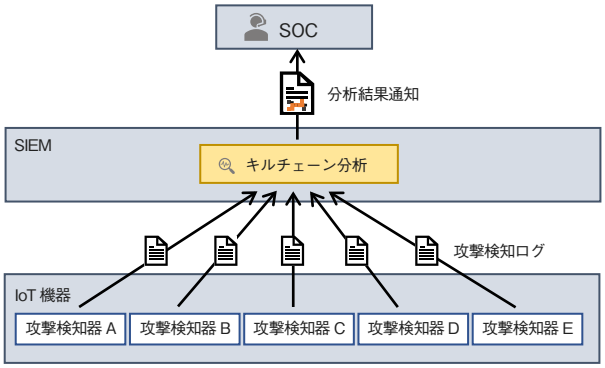
4. キルチェーン分析技術

4.1 インシデント分析における課題

前章で述べた攻撃検知技術は，制御ネットワーク上の各ノードにおける攻撃を検知する技術であった．しかし，実際の攻撃は単一のノードで完結することはなく，ネットワークの侵入口ノードから攻撃対象のノードまで，各ノードに攻撃が行われる（以降，この一連の攻撃行動を攻撃シナリオと呼ぶ）．

この攻撃シナリオに対して，攻撃リスクを評価するには，侵入経路や攻撃フェーズの特定が必要であるが，単一のノードにおける攻撃検知結果のみでは，その分析に不十分である．そのため，各ノードから収集した複数の攻撃検知結果から俯瞰（ふかん）的に分析を行うキルチェーン分析技術が必要となる[10]．しかし，各ノードから攻撃検知結果を収集したとしても，実際には，全てのフェーズで攻撃を検知できるとは限らず，未検知や誤検知によって，侵入経路などの全容の特定が困難なケースが存在する．

そこで，筆者らは複数の攻撃検知結果から攻撃を受けたノードを特定し，侵入経路や攻撃リスクを判定するキルチェーン分析技術を研究している．**第7図**では，インシデント分析におけるキルチェーン分析技術の位置づけを示している．このキルチェーン分析技術はSIEM上に搭載し，各ノードから収集した攻撃検知結果を総合的に分析することで，侵入経路や誤検知の有無，攻撃シナリオの推定などの分析を実現する．さらに，キルチェーン分析に基づくインシデントのトリアージによって，より効率的な対応・復旧が期待できる．



第7図　IoTセキュリティのインシデント分析技術
Fig. 7　Incident analysis technology for IoT security

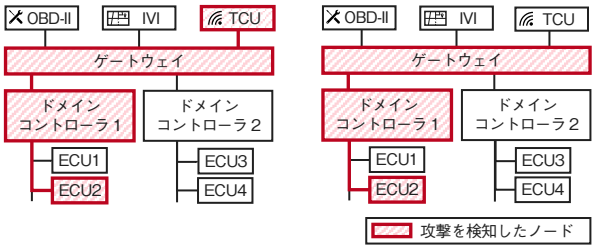
4.2 車載ネットワークに対するキルチェーン分析技術

本節では，具体的な事例として，車載ネットワークに対するキルチェーン分析技術について述べる．

自動車の車載ネットワークは，複数のECU（Electronic Control Unit）が接続されており，これらのECUが車両制御や情報通信などの機能を実現している．この車載ネットワークにおける攻撃検知結果と侵入経路の例を**第8図**に示す．図中のOBD-II（On Board Diagnostic-II）は自動車に搭載される診断ポート，IVI（In-Vehicle Infotainment）は車載インフォテイメントシステム，TCU（Telematics Control Unit）は車外との通信ユニットを指す．まず，侵入経路が明らかな例を**第8図（a）**に示す．このケースは車載ネットワーク上を数珠つなぎに最深部まで侵入されており，その攻撃リスクは高いと判断できる．一方で，侵入経路が明らかではない例を**第8図（b）**に示す．このケースはOBD-II，IVI，TCUの第1層目において，いずれのノードも攻撃を検知していないことから，どのノードが攻撃の侵入口ノードであるかを判別できず，侵入経路も特定できない．この例のように，攻撃検知結果が正確ではないケースの判定が，侵入経路判定の課題である．

この課題に対し，筆者らは車載ネットワーク上の攻撃検知結果に加え，車両の制御情報や通信状態などのセキュリティとは無関係な二次情報を用いて，侵入経路を判定する技術を研究している[11]．この技術では，**第8図（b）**のような場合において，斜線部のノードで攻撃を検知する直前に，TCUから新規のサーバとの通信など，攻撃により起こり得る挙動があったノードを攻撃の侵入口ノードとして判定する．このように，攻撃により副次的に生じる挙動を活用することで，**第8図（b）**のような侵入口ノードの未検知に限らず，誤検知などのケースでも侵入経路特定が期待できる．

本稿では，車載ネットワークを例に説明したが，本技術は工場や制御ネットワークなどの複雑なネットワーク環境へも応用できる．



(a) 侵入経路が明らかな例　(b) 侵入経路が明らかではない例

第8図　車載ネットワークにおける攻撃検知と侵入経路
Fig. 8　Attack detection and intrusion path on an in-vehicle network

5. SOCによる制御システムの監視サービス

本節では，制御システムの監視における課題と，制御システムの一例である工場のSOCサービスで実施される対策や運用例について述べる．

5.1 制御システムの監視における課題

制御システムのセキュリティ監視では，その性質上ITシステムのセキュリティ監視とは異なり，下記に挙げる課題が生じる．

(1) ライフサイクルはITシステムでは3～5年程度であるが，制御システムでは10～30年であるためOSサポート終了後もシステムが稼働し続けることがある．
(2) 制御システムは専用装置が多くITシステムで導入されるエンドポイントでの監視・対策が困難である．
(3) 資産管理やそれに基づくリスク特定が不十分な場合が多く一度被害が発生すると，被害の範囲の特定や抑え込みが困難である．
(4) 制御システムでは可用性が重視されるため，システムの一部切り離しなどのITシステムで通常取られる対策が取れないことがある．

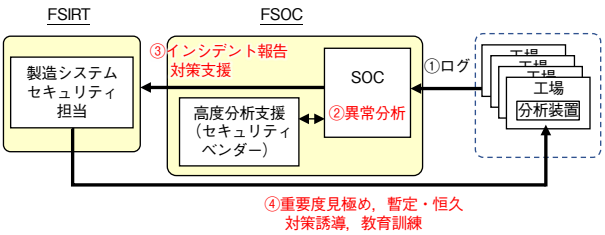
5.2 工場 SOC での対策と運用例

課題(1)，(2)に挙げられるように，制御システムではエンドポイントのセキュリティ対策の導入が困難である．そこでパナソニックの工場では，セキュリティ対策としてパッシブにネットワークを監視する方法を採用している．収集されたネットワークログは，分析装置による異常検知が施され，検知された異常に対してセキュリティ分析官が詳細分析を行う．

課題(3)，(4)は，導入する異常検知システムやSOCのセキュリティ分析官の知見だけでは必ずしも解決できる問題ではない．そこで有事の際には製造システムセキュリティ担当部門（Factory SIRT）を交えて現場と連携しながら影響範囲の特定や適切な対処法を検討する．

これらを踏まえ，当社工場のSOCによる異常検知サービスでは以下のような手順にて異常を検知し，セキュリティインシデントに対応する．

(1) 監視に先立ち，リスクアセスメントを通じて重要資産の抽出，脅威シナリオの策定を行い，製造システム内に存在するリスクの特定と評価を行う．
(2) スイッチングハブからミラーリングした通信データを蓄積し分析する．既知の脆弱（ぜいじゃく）性攻撃の検出や，工場端末の振る舞いをアプリケーションレベルまで分析した結果をIoT-SIEMへ送信する．
(3) 工場端末の振る舞いデータから操業パターンをAIで学習し，サイバー攻撃の初期段階で異常を捉える．また，外部の最新のスレットインテリジェンスを活用して異常な振る舞いを検知する．
(4) IoTを理解したセキュリティ分析官が，日々検出される異常アラートを分析し，リスク評価を行う．
(5) インシデント認定時，セキュリティ分析装置のパケットキャプチャデータを元に攻撃成功の有無確認などを実施し，リスクの評価結果に基づいた工場の緊急停止の必要性を製造システムセキュリティ担当部門と議論し，必要であれば復旧を支援する．



FSIRT：Factory Security Incident Response Team
FSOC：Factory Security Operation Center

第9図 工場SOCサービス
Fig. 9 Factory SOC service

6. まとめ

本稿では，攻撃を可視化し分析するためのSIEMを用いたIoTサイバーセキュリティシステムについて述べ，そこで用いる IoT機器へのサイバー攻撃に特化したAIによるサイバー攻撃検知技術を提案し，その有効性を示した．また，攻撃リスクを正確に評価するために，侵入経路や攻撃フェーズを特定するキルチェーン分析技術について提案した．最後に，当社工場SOCサービスの課題と対策について紹介した．当社の工場SOCについてサービスの運用実績をベースに，自動車，ビル，ホームへ監視対象範囲を拡（ひろ）げ，IoT時代における安心・安全な社会の実現に貢献する．

参 考 文 献

[1] C. Miller et al., “Remote Exploitation of an Unaltered Passenger Vehicle,” DEF CON, Las Vegas, July 2015.
[2] UNECE, “UN Regulation No.155-Cyber security and cyber security management”, https://unece.org/transport/documents/2021/03/standards/u n-regulation-no-155-cyber-security-and-cyber-security, 参照 Oct. 20, 2021.

[3] ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第1版, 経済産業省, 2019.
[4] スマートホームの安心･安全に向けたサイバー･フィジカル･セキュリティ対策ガイドライン, 経済産業省, 2021.
[5] T. Haga et al., “Automotive SIEM and Anomaly Detection using Sand Sprinkled Isolation Forest,” Embedded Security in Cars, Berlin, Nov. 2017.
[6] T. Oba et al., "Graph Convolutional Network-based Suspicious Communication Pair Estimation for Industrial Control Systems". arXiv preprint arXiv:2007.10204, 2020.
[7] R. R. R. Barbosa et al., “Flow whitelisting in SCADA networks,” International Journal of Critical Infrastructure Protection (IJCIP), vol. 6, no. 3-4, 2013.
[8] K. Stouffer et al., “Guide to industrial control systems ICS security,” NIST special publication, vol. 800, no. 82, 2011.
[9] M. Schlichtkrull et al., “Modeling relational data with graph convolutional networks,” in Proc. of Extended Semantic Web Conference (ESWC), June 2018.
[10] E. Hutchins et al., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Leading Issues in Information Warfare & Security Research. 1, Jan. 2011.
[11] H. Tasaki et al., “Attack Analysis Level and Attack Route Determination for Vehicle Remote Monitoring System,” Symposium on Cryptography and Information Security, Jan. 2021.
[12] J. Tang et al., “Line: Largescale information network embedding,” International World Wide Web Conference (WWW), May, 2015

執筆者紹介

芳賀　智之　Tomoyuki Haga
テクノロジー本部　デジタル・AI技術センター
Digital & AI Technology Center, Technology Div.

大庭　達海　Tatsumi Oba
製品セキュリティセンター
サイバーセキュリティ技術開発部
Cyber Security Technology Development Department, Product Security Center

田崎　元　Hajime Tasaki
テクノロジー本部　デジタル・AI技術センター
Digital & AI Technology Center, Technology Div.

鴨川　郷　Akira Kamogawa
製品セキュリティセンター
サイバーセキュリティ技術開発部
Cyber Security Technology Development Department, Product Security Center

佐々木　崇光　Takamitsu Sasaki
製品セキュリティセンター
サイバーセキュリティ技術開発部
Cyber Security Technology Development Department, Product Security Center

松島　秀樹　Hideki Matsushima
製品セキュリティセンター
サイバーセキュリティ技術開発部
Cyber Security Technology Development Department, Product Security Center