

ジャパンデータストレージフォーラム (JDSF)

2019 新春セミナー

# 待ったなしのセキュリティ対策 ～ 新たな流れ ～

**TOSHIBA**

東芝デジタルソリューションズ株式会社

2019年2月1日

# Contents

01 動向

02 基本的な考え方

03 新たな流れ

～ マルウェア対策

～ システム可用性維持のための対策

01

# 動 向

# 攻撃者と目的と環境

## [攻撃者]

- 犯罪者／犯罪グループ、諜報員／産業スパイ、ハッカー集団、悪意ある組織の職員（退職者を含む）など
- 攻撃者の**低年齢化**が顕著な傾向

## [攻撃の目的]

- **金銭盗取（事後販売などの間接的なものを含む）**
- **産業スパイ活動（機密情報）**
- **国家や企業などの戦略変更やイメージダウンを狙う組織犯罪**
- ハクティビストによる政治的・社会的な主張
- 愉快犯（自己満足） など

## [環境]

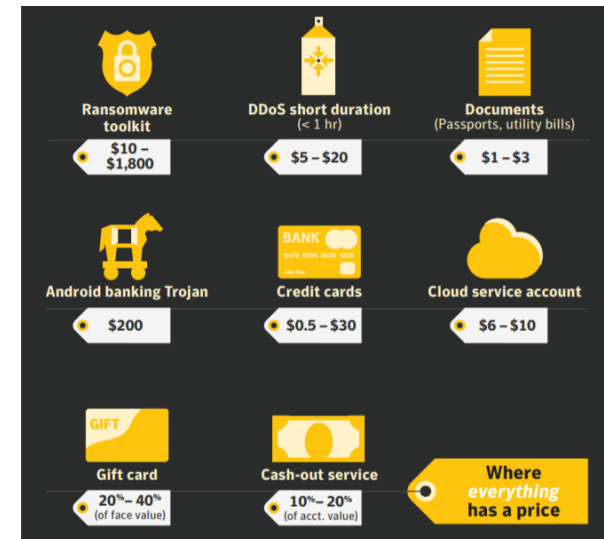
- 攻撃のビジネス化（**アンダーグラウンドサービス**）（※ RaaS、PhaaS、CaaS）
  - ✓ 素人の依頼に基づくプロによる攻撃
- **攻撃ツールのコモディティ化**
  - ✓ 攻撃者にスキル（知識・ノウハウ）は必要ない
- 組織的、分担作業

(例)

プロによる安価な  
DDoS攻撃サービス

料金

1～4時間：2ドル／H  
5～24時間：4ドル／H  
24～72時間：5ドル／H  
1か月：1,000ドル



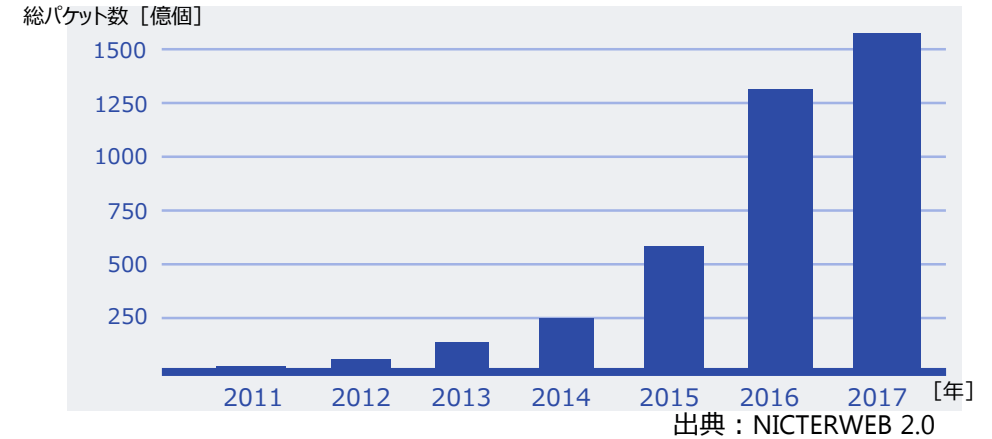
※ RaaS (Ransomware-as-a-Service)  
PhaaS (Phishing-as-a-Service)  
CaaS (Crimeware-as-a-Service)

# セキュリティの攻撃量と傾向

## 日本への攻撃パケットが急速に増加

NICTER(※)が観測する年間総観測パケット数

※情報通信研究機構(NICT)が開発したサイバー攻撃トラフィックの観測／分析システム



## 攻撃の傾向 ～「情報セキュリティ10大脅威」

順位	「組織」の10大脅威 2017年	2016年 順位	「組織」の10大脅威 2018年	2017年 順位
1位	標的型攻撃による情報流出	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	7位	ランサムウェアによる被害	2位
3位	ウェブサービスからの個人情報の搾取	3位	ビジネスメール詐欺	ランク外
4位	サービス妨害攻撃によるサービスの停止	4位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
5位	内部不正による情報漏洩とそれに伴う業務停止	2位	セキュリティ人材の不足	ランク外
6位	ウェブサイトの改ざん	5位	ウェブサービスからの個人情報の搾取	3位
7位	ウェブサービスへの不正ログイン	9位	IoT機器の脆弱性の顕在化	8位
8位	IoT機器の脆弱性の顕在化	ランク外	内部不正による情報漏えい	5位
9位	攻撃のビジネス化(アンダーグラウンドサービス)	ランク外	サービス妨害攻撃によるサービスの停止	4位
10位	インターネットバンキングやクレジットカード情報の不正利用	8位	犯罪のビジネス化	9位

出典：独立行政法人 情報処理推進機構 (IPA)  
「情報セキュリティ10大脅威(組織編)」より  
<https://www.ipa.go.jp/security/vuln/10threats2018.html>

# 攻撃は止まらない

ビジネス | xTECH | クロストrend | 医療 | TRENDY | WOMAN | ショッピング | 転職 | ナショジオ | 日経電子版 | 日経BP

2018年4月4日 (水)

TOP | 小売り・サービス | 情報・通信 | 製造 | 政治・経済・国際 | スキル・ライフ | テーマ特集

総合トップ > 政治・経済・国際 > ニュースを斬る

ニュースを斬る

## コインチェック、仮想通貨580億円消失のその後

「補償」と「事業継続」でも信頼回復は茨の道

バックナンバー

2018年1月29日 (月)

仮想通貨取引所大手のコインチェック（東京・渋谷）は1月26日、利用者から預かっている約580億円相当の仮想通貨「NEM」を外部からの不正アクセスによって失ったと発表した。2014年に「マウントゴックス」が約470億円分を消失させてから、最大の仮想通貨の流出案件となった。

コインチェックがNEMの入出金や売買を一時停止し始めたのは、同日昼ごろのこ

> ニュース > 製品・サービス

## ボーイングに「WannaCry」ランサムウェア被害と報道--影響は限定的

Steven Musil (CNET News) 翻訳校正：編集部 2018年03月29日 10時17分

シェア 21 | ツイート | BI 17 | Pocket 38 | G+ | 印刷 | メール | 保存 | クリップ

[The Seattle Times](#)によると、Boeingが米国時間3月28日、ランサムウェア「WannaCry」の被害に遭い、製造への影響が一時懸念されたが、同社は後に製造への影響はないとの声明を出した。

The Seattle Timesによると、今回の感染は、Boeing Commercial Airplaneの製造エンジニアリング部門でチーフエンジニアを務めるMike VanderWel氏が送信したメモの中で明かされ、VanderWel氏は「全員の協力」を要したと述べた。

VanderWel氏は、「それはノーコード化された桁組み立てツール」が飛行機の機能性テストで使われる機器に感染していると伝えた。

関連ジャンル | セキュリティ戦略 | 標的型攻撃 | セキュリティ総論

## スタバも被害に…「仮想通貨をマイニングさせる」マルウェアは地味に危険

コインチェックに続き、イタリアのBitGrailでも180億円以上のNanoコインが不正に送金されるなど、立て続けに巨額の不正送金で揺れる仮想通貨界隈。取引所のサイバー攻撃や詐欺が大きな問題になっているが、地味に続く仮想通貨周辺のサイバー攻撃に「マイニング（採掘）マルウェア」がある。2017年春ごろからセキュリティベンダーなどに確認され、その後も攻撃は続いている。直接の金銭被害はないが、派生するリスクは無視していいものではない。

## 盗まれるもの

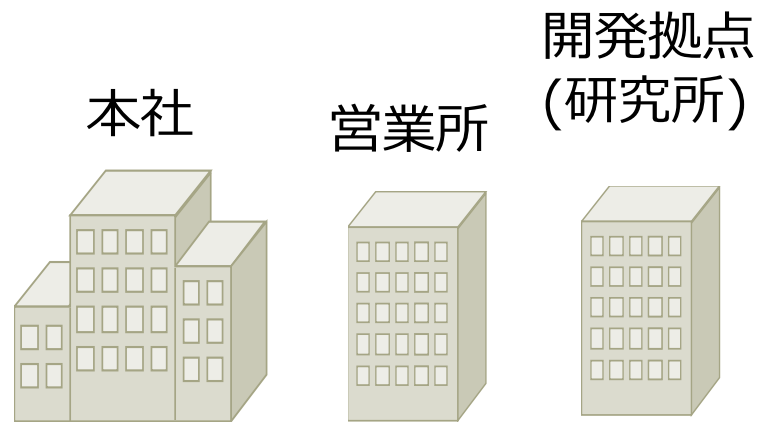
# 金銭（直接的／間接的）、コンピュータリソース

出展：  
<http://business.nikkeibp.co.jp/atcl/report/15/110879/012800779/>  
<https://japan.cnet.com/article/35116877/>  
<https://www.sbbit.jp/article/cont1/34589>

# 攻撃ターゲット

- 攻撃目的が【金銭盗取、産業スパイ活動】  
(リスク) 情報漏洩（情報盗取&売却）や ランサムウェア等を用いた脅しによる金銭要求。攻撃ターゲットは、ほぼ**ITシステム**。  
(対策) **マルウェア対策**
- 攻撃目的が【国家や企業などの戦略変更やイメージダウンを狙う組織犯罪】  
(リスク) システム停止／破壊。攻撃ターゲットは、**OTシステム**。  
(対策) **システム可用性維持のための対策**

IT : Information Technology  
OT : Operational Technology



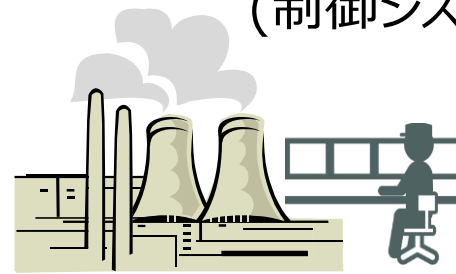
**ITシステム : マルウェア対策**

生産拠点 (工場)



**OTシステム : システム可用性維持対策**

産業システム (制御システム)



対策優先度  
ITシステム : CIA  
OTシステム : AIC  
C : Confidentiality  
I : Integrity  
A : Availability

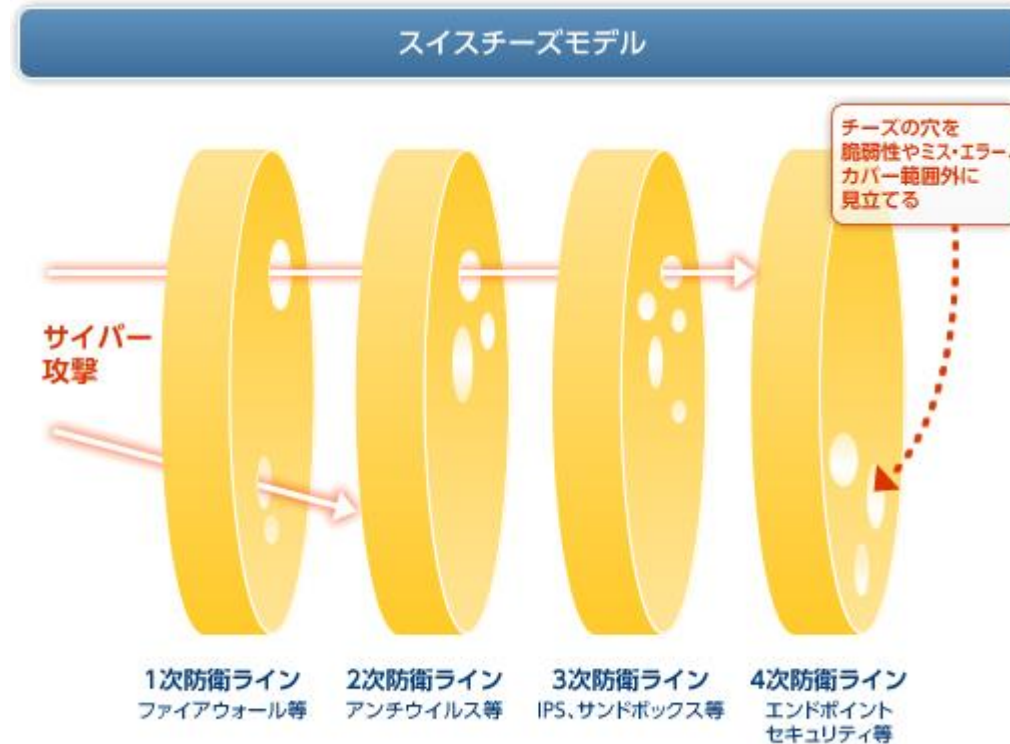
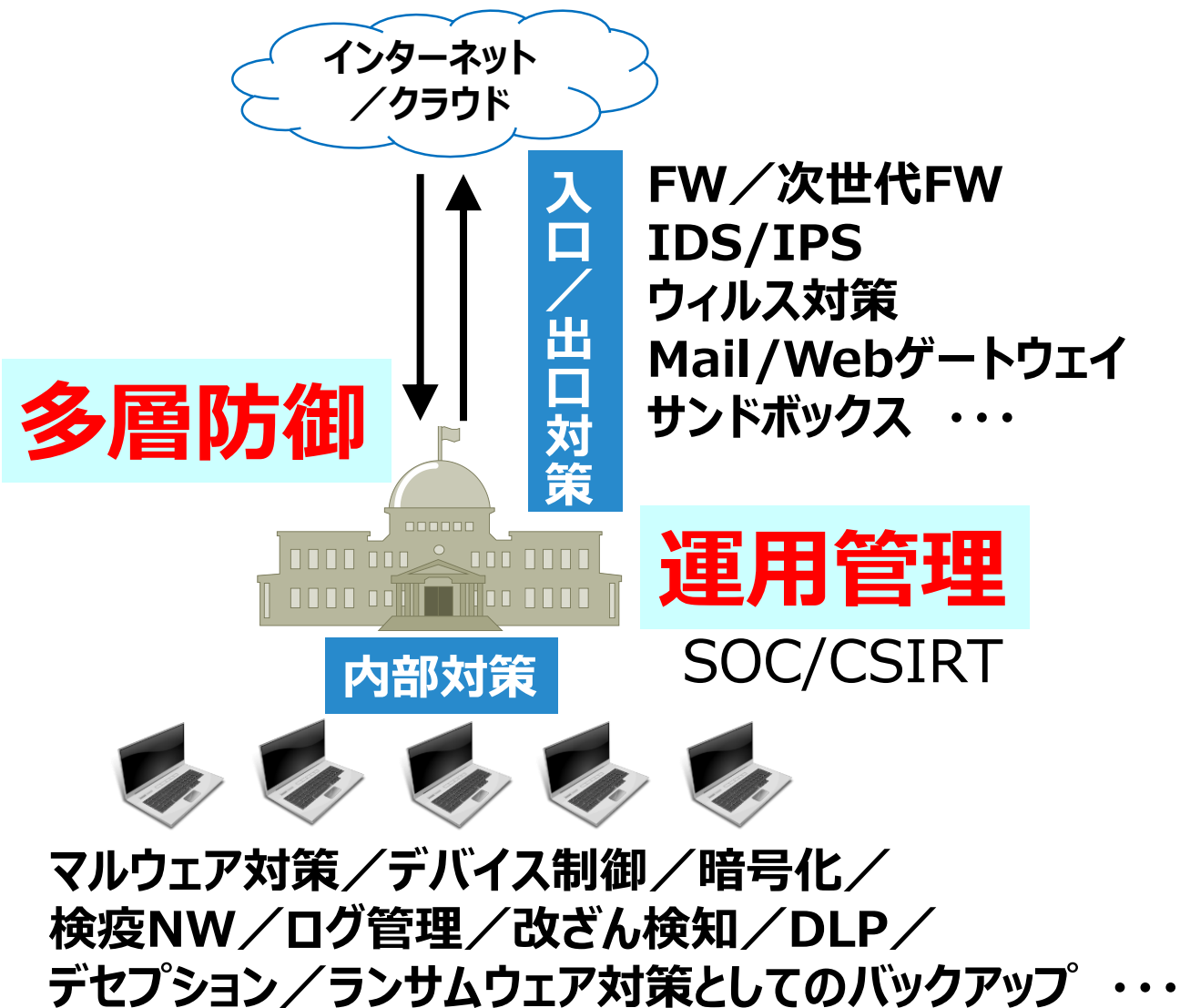
# 02

## 基本的な考え方



# 多層防御と運用管理

## 入口/出口対策、内部対策と運用管理



[多層防御の意義は]

- 視点の異なる防御策を何重にも組み合わせることで侵入や漏洩の**リスクを低減**
- 侵入を遅らせることで被害に至る前に防御側がサイバー攻撃に**気付く効果**

# 気付く効果 ～ 攻撃のステップ

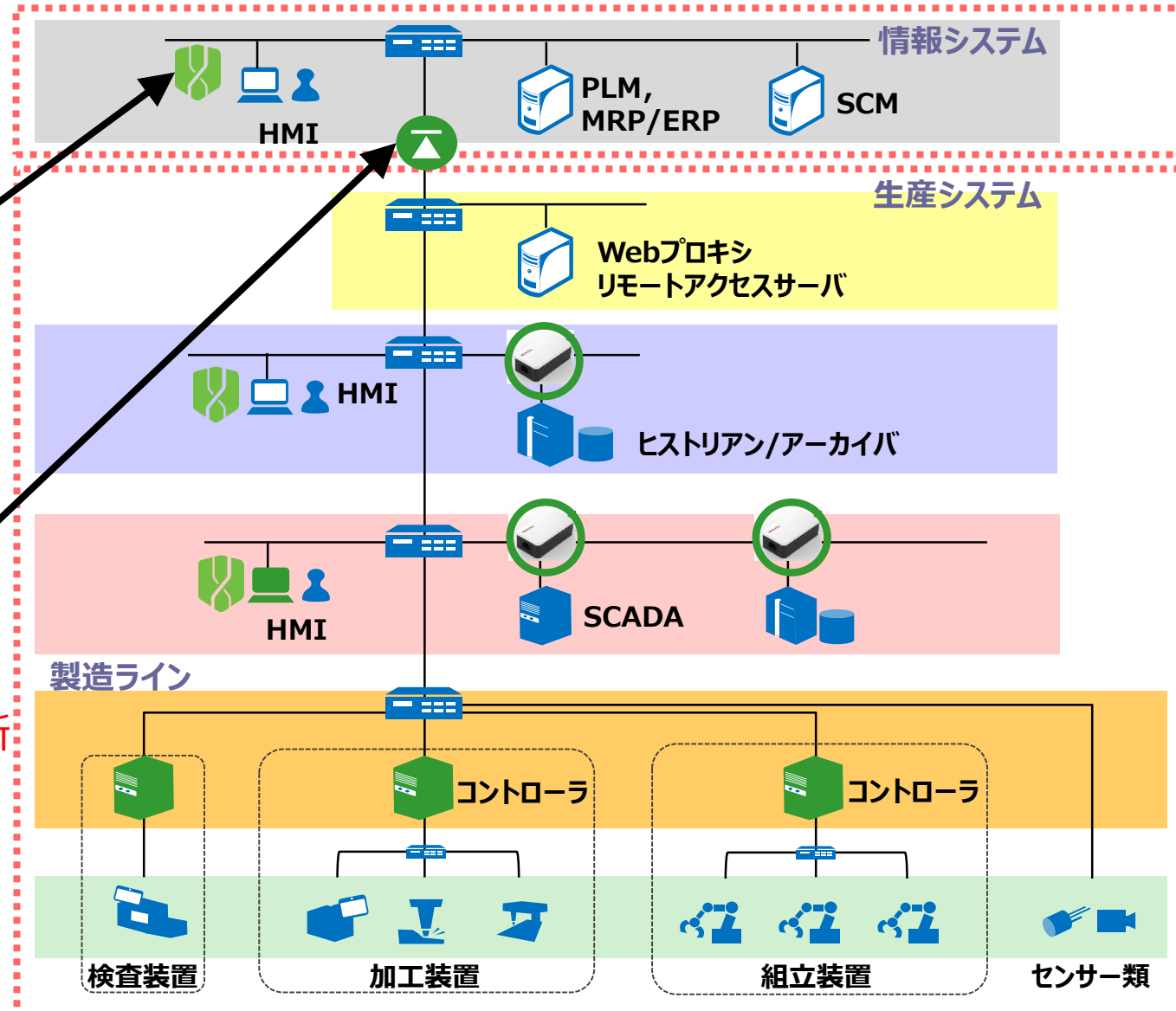


多層防御で複数の壁を作り、侵入・目的達成のための時間をかけさせる。  
並行して、運用管理の中で、もがいている攻撃者の動きに気付く！

03

# 新たな流れ

# 新たな流れ = 尖った機能



ITシステム

OTシステム

**CylancePROTECT®**  
Artificial Intelligence. Real Threat Prevention.  
次世代マルウェア対策ソフトウェア

AIを利用した脅威的な検知率

**WATERFALL®**  
Stronger Than Firewalls  
外部からの通信を物理的に遮断  
する一方向セキュリティゲートウェイ

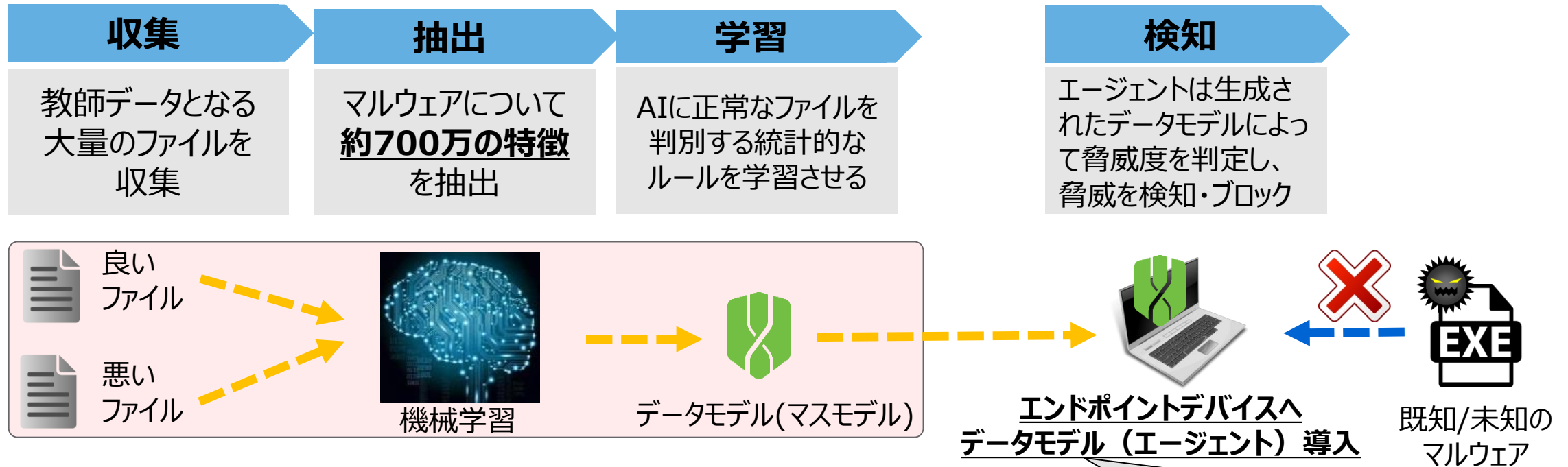
外部からの通信を物理的に遮断

# マルウェア対策 ～ CylancePROTECT ～

# 次世代マルウェア対策ソフトウェア CylancePROTECT



機械学習により生成したデータモデル（AIモデル）でファイルの特徴点を解析  
パターンファイルに依存することなく、既知/未知のマルウェアを検知



# CylancePROTECT の特長

## ■ AIモデル（データモデル）による**高い検知率（99.7%）**（※） Cylanceによる測定結果

- 既知・未知マルウェアを意識することなく高精度で検知・ブロック

## ■ **実行前防御**

- カーネルからプログラムの実行指令が出たタイミングでフックして判定

## ■ **シグネチャ／パターンファイルが存在しない**

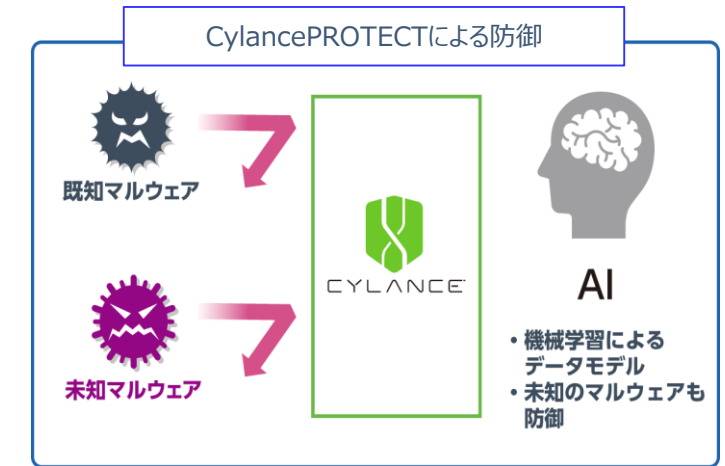
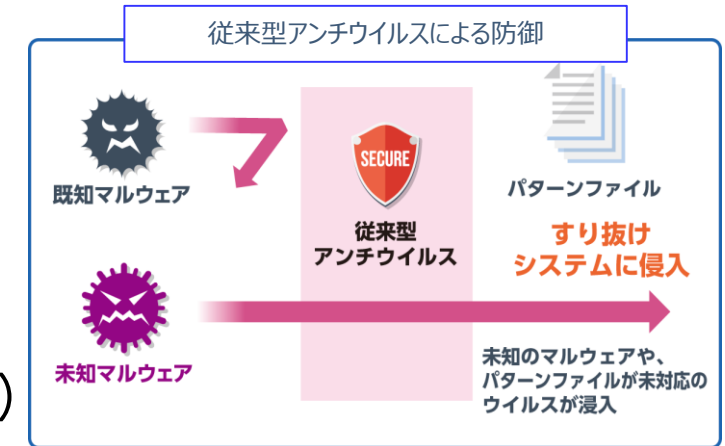
- 日々のシグネチャ／パターンファイルのアップデート不要（**管理者の負荷軽減**）
- 定期スキャンが不要（**利用者の負荷軽減**）
- インターネット接続が無い環境にも適用可能

## ■ **適用範囲が広い**

- スタンドアロン環境、サーバの塩漬け・延命措置も可能（一部のOSに限定）

## ■ **動作が軽い**

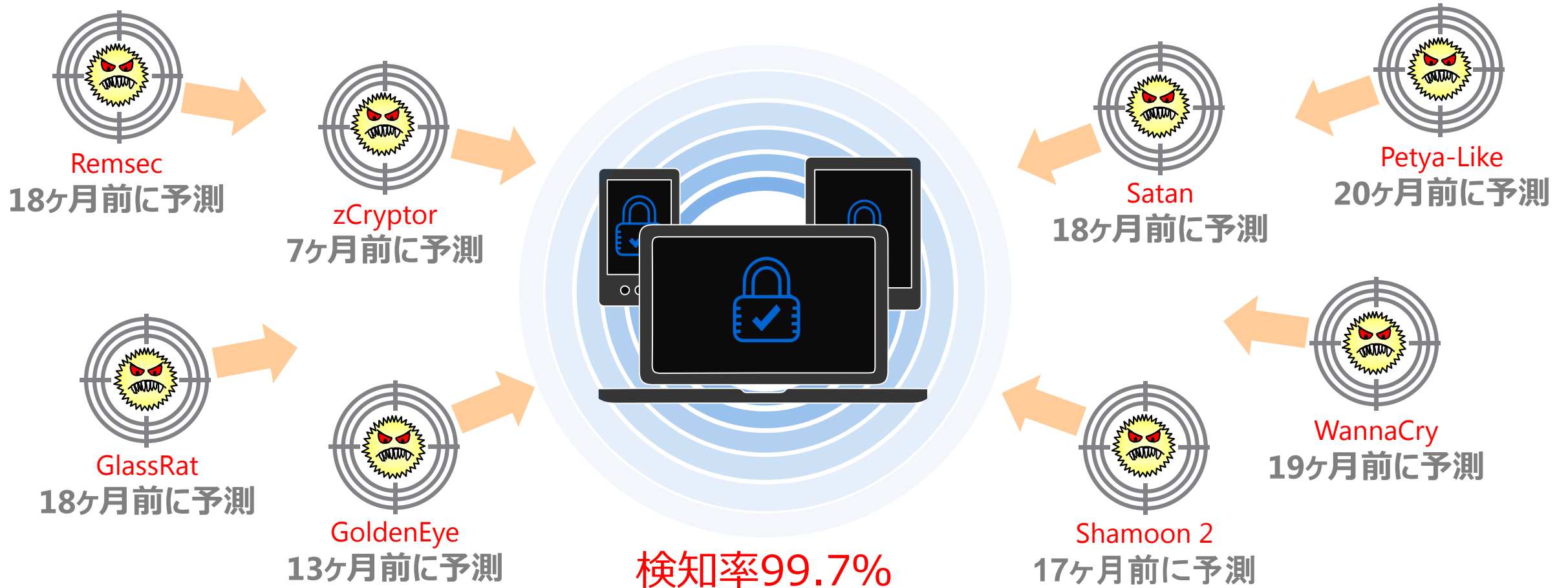
- 動作機構上、システム負荷が軽い（**業務効率向上**）
- 管理機能がクラウドで提供されるためオンプレミスの管理サーバが不要（**運用管理コスト低減**）



# ずばぬけた検知能力

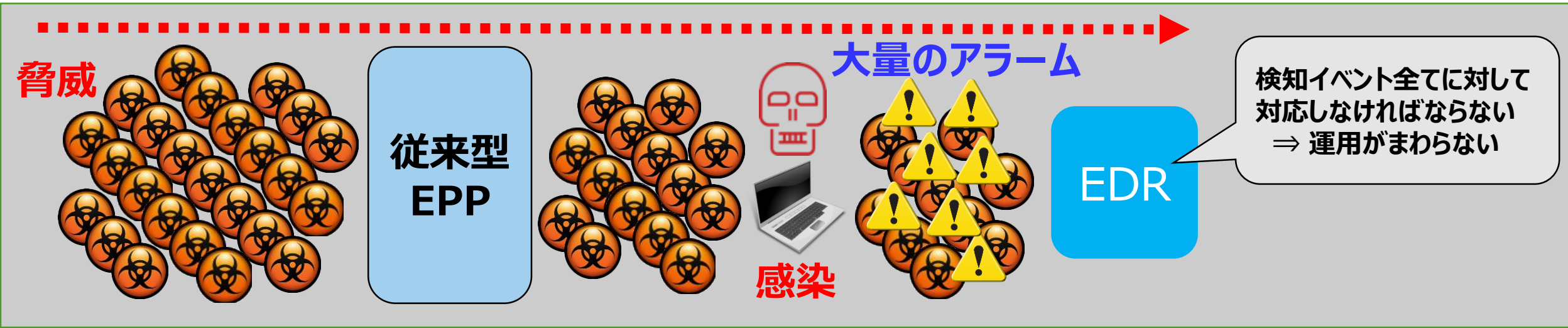
～ 実際の脅威が現れる前に予測した数多くの実績

Cylance が作成したデータモデルは WannaCry をはじめとする  
数多くの脅威を数ヶ月以上前から予測して防御しています





# EPP(Endpoint Protection Platform) と EDR(Endpoint Detection and Response)



# システム可用性維持のための対策 ～ Waterfall ～

# 制御システム（OTシステム）を取り巻く環境

国民生活や社会経済活動に重大な影響を及ぼさないことを目的として重要インフラ防護の行動計画が策定

サイバーセキュリティ戦略本部により、14分野が指定されています



引用: <https://www.nisc.go.jp/active/infra/outline.html>

汎用OS・プロトコル採用や、外部ネットワークへの接続など、制御システムの環境が変化

## クローズドから外部接続へ

- ✓IoTによる業務系接続増加
- ✓操業データ活用/提示

## 制御システムの汎用化・IT化

- ✓Win/Linuxの汎用OS採用
- ✓TCP/IPプロトコル採用

## 制御システムが攻撃対象に

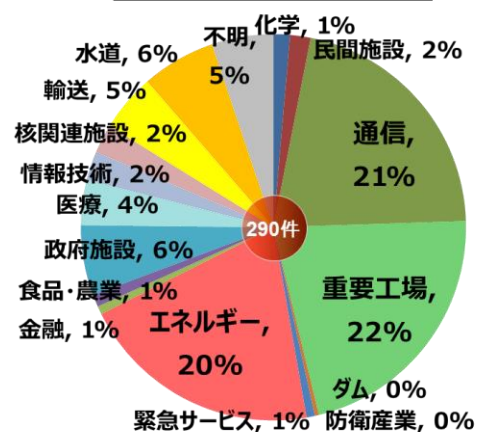
- ✓制御関連セキュリティ事故増大
- ✓制御機器脆弱性発見数増大

## 標準化/規制化状況

- ✓認証制度(CSMS/EDSA)
- ✓標準化/ガイドライン整備

## インシデントは増加傾向

セクター別の割合（2016年度）



米ICS-CERTインシデント統計（米会計年度別）



## 一方でセキュリティ対策は旧来のまま

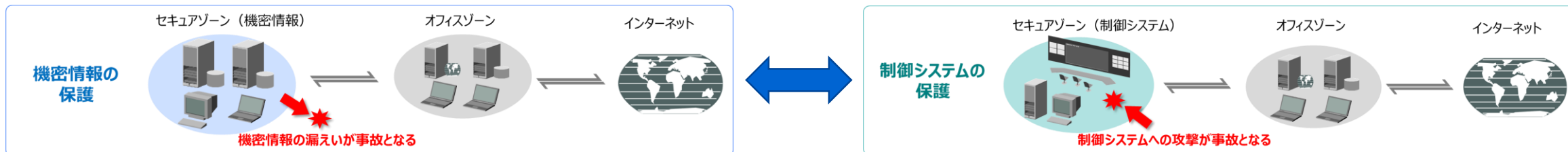
- クローズド環境を前提としており、ネットワークおよびエンドポイントのセキュリティ対策は実施できていない。
- 可用性優先で(システムを停止することが出来ず)セキュリティパッチを適用できない。
- 防止策だけでなく検知策も無いため、サイバー攻撃の被害を受けているかわからない。

セキュリティインシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故を指す


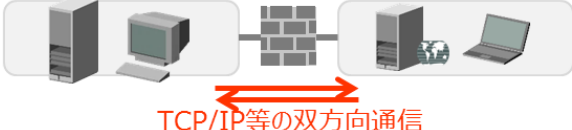

引用: [http://mscs2018.sice-ctrl.jp/program/\\_tutorials/mscs2018tutorial\\_abe.pdf](http://mscs2018.sice-ctrl.jp/program/_tutorials/mscs2018tutorial_abe.pdf)

# ネットワークゾーニングの重要性

ネットワークゾーニングとは、セキュリティ管理のためにセキュリティレベルの異なるネットワークを分離して通信を制限すること



## 一方向通信によるゾーニングを推奨

種別	概要	特徴
物理分割	物理的隔離（電氣的な接続が無い） エアギャップ（空気の隙間）がある 	<ul style="list-style-type: none"> <li>○ 物理的にネットワーク分離できる</li> <li>× データ授受が必要な場合、運用が煩雑になる（USB等メディアの管理）</li> </ul>
論理分割	物理的な「接続」を行った上で、ファイアウォール等でTCP/IPの論理的な通信制御を行う 	<ul style="list-style-type: none"> <li>○ 比較的安価に実現できる</li> <li>× セキュリティ上の懸念が拭い去れない</li> </ul>
一方向通信	物理的隔離の上で、一方向にだけ光通信によるデータ伝送経路を持たせる 	<ul style="list-style-type: none"> <li>○ 制御システムを確実に守りつつ、一方向通信を実現できる</li> <li>× 比較的高価となる</li> </ul>

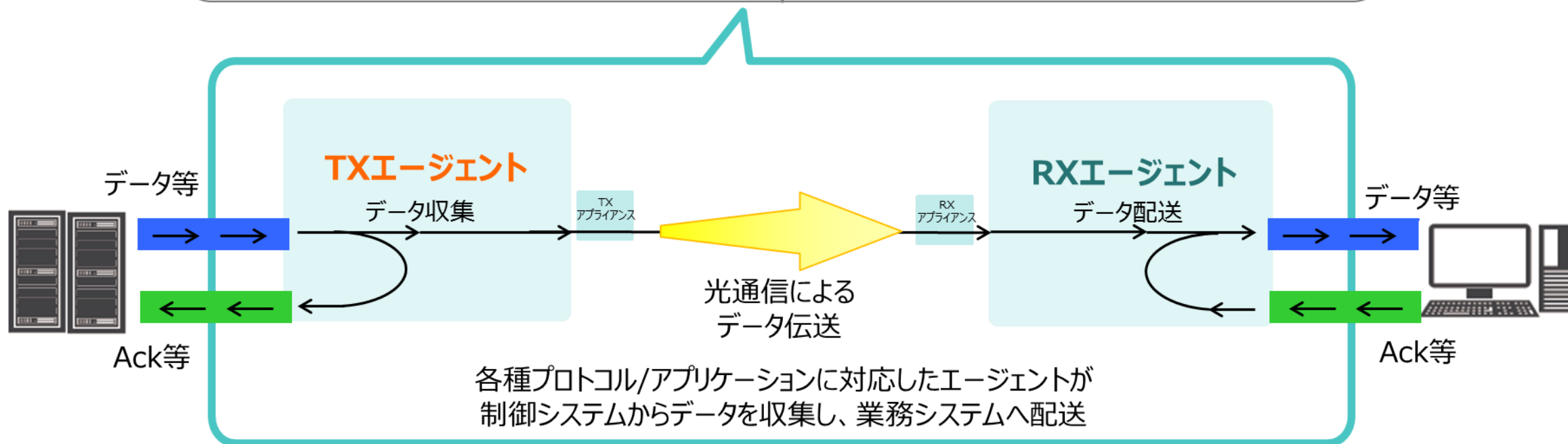
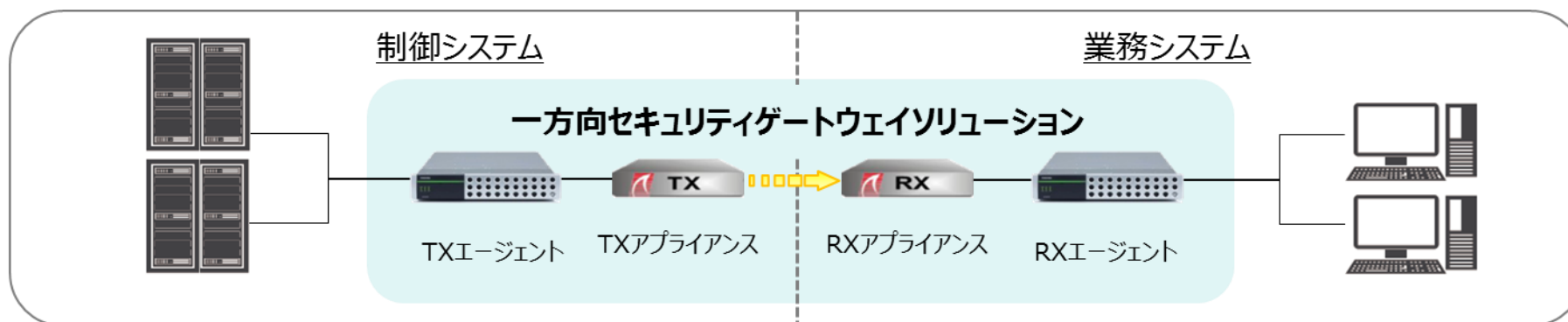
# 一方方向セキュリティゲートウェイとは

物理的な一方方向通信を実現するセキュリティアプライアンス

サイバー攻撃から保護された環境で、重要システムの各種データを活用することが可能



# 一方方向セキュリティゲートウェイ ～シームレスな既存システム接続



# Waterfallエージェント ～対応アプリケーション/プロトコルの例

Waterfall社は複数のICSプロダクトベンダーとパートナーシップを締結しており、多様なプロトコルに対応したWaterfallエージェント（Waterfallコネクタ）を提供

## 主要な産業アプリケーション/ヒストリアン 主要な産業プロトコル

- OSisoft PI, PI Asset Framework
  - GE iHistorian, GE iFIX, GE OSM
  - Siemens WinTS
  - Emerson Ovation, Wonderware Historian
  - **MS SQLServer, Oracle DB,** MySQL, Postgres
  - AspenTech IP21, Matrikon Alert Manager
  - Schneider ClearSCADA
- OPC: **DA**, HDA, A&E, UA
  - DNP3, ICCP, Modbus
  - IEC60870-5-104

## リモートアクセス

- Remote Screen View

## ITコネクタ

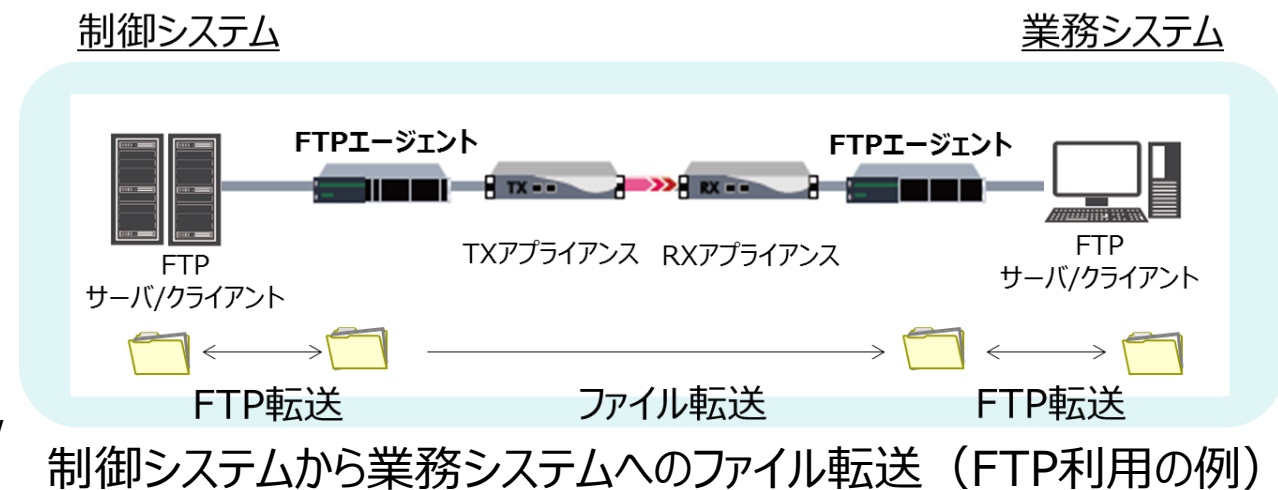
- **UDP, TCP/IP**
- **NTP**, Multicast Ethernet
- IBM MQ series, Microsoft MSMQ
- Antivirus updater, patch (WSUS) updater
- Remote print server

## 主要なIT監視アプリケーション

- **SNMP, SYSLOG**
- Splunk, McAfee ESM SIEM, HP ArcSight SIEM
- CA Unicenter, CA SIM, HP OpenView

## ファイル/フォルダミラーリング

- **FTP, TFTP, SFTP, FTPS, RCP**
- **remote folders (CIFS), Local Folder,** tree mirroring



# Waterfall冗長構成 (HA:High Availability,高可用性対応)

Waterfallでは、TX/RXを2セットを組み合わせて、冗長(HA)構成とすることも可能です

## WF-400 TX/RX

(対応エージェントのみ)



### Waterfall冗長構成 (構成概要)

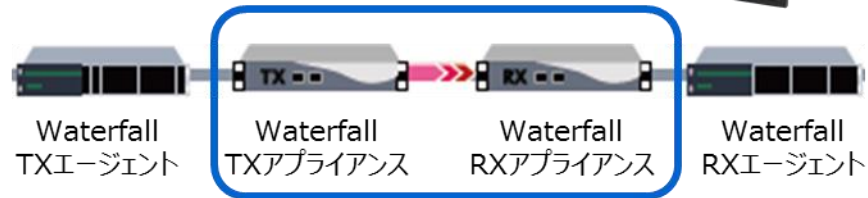
- ✓ 冗長構成は、TX/RXエージェントサーバのクラスタリング構成がベースとなる (Active/Passive)
- ✓ TX/RXエージェントサーバには、計4枚のNICが必要 (うち2枚はWaterfallアプライアンス2台との接続用)
- ✓ 2組のWaterfall TX/RXアプライアンスと2組のTX/RXエージェントをイーサネットケーブルでそれぞれ接続



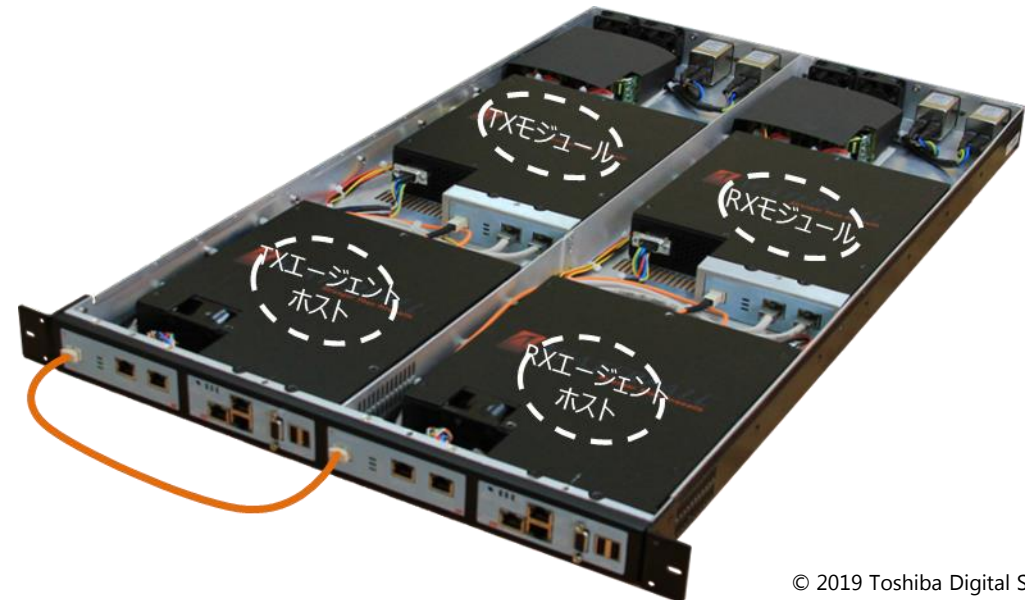


# Waterfall一方向セキュリティゲートウェイ ～2つのモデル

## WF-400 (基本モデル、冗長構成に対応)



## WF-500C (オールインワンモデル)



# TOSHIBA

※Cylance および CylancePROTECTは、米国および諸外国における Cylance Inc. の登録商標または商標です。

※Waterfall一方方向セキュリティゲートウェイ（Waterfall's Unidirectional Security Gateway）の開発元は、Waterfall Security Solutions Ltd.です。

※Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

※本記載の社名および商品の名称はそれぞれ各社が商標または登録商標として使用している場合があります。

本資料に表記されている数値および表現は2019年 1月現在のものです。

本資料の内容は、予告なく変更する場合があります。詳細は、仕様書あるいは説明書をご覧ください。