サプライチェーンセキュリティを向上させるための4つの転換点と先進例

門林 雄基
奈良先端科学技術大学院大学
サイバーレジリエンス構成学研究室
2019/11/7

背景：偽部品の脅威

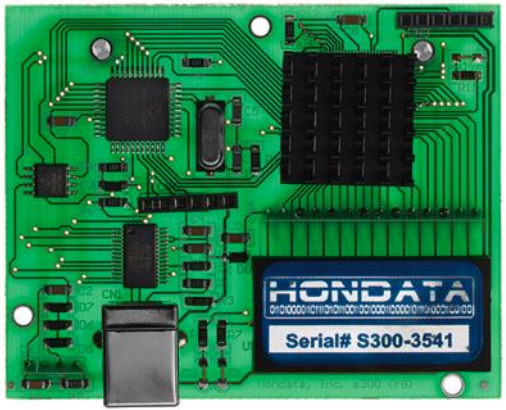
IEEE SPECTRUM Topics Reports Blogs Multimedia

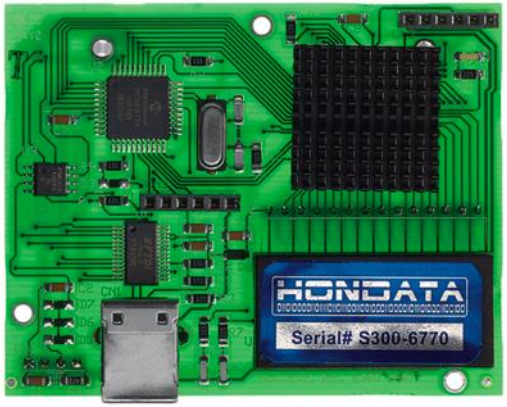
Feature | Computing | Hardware

24 Apr 2017 | 15:30 GMT

Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market

Fake hardware could open the door to malicious malware and critical failures





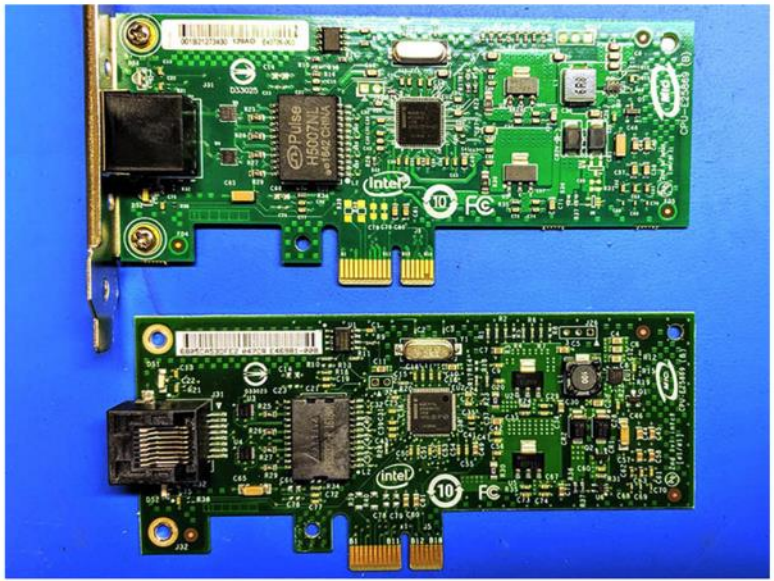
Source:
IEEE Spectrum

背景：偽部品の脅威

Identifying Risky Counterfeit Intel Gigabit CT Network Adapters

By **Patrick Kennedy** - July 11, 2019 15

いいね！ 33 Tweet



Counterfeit And Real Intel Gigabit CT Desktop Adapters Cover

Source:
www.servethehome.com

背景： バックドアの脅威

JavaScript

Reported malicious module: getcookies

Early May 2nd, the npm security team received and responded to reports of a package that masqueraded as a cookie parsing library but contained a malicious backdoor. The result of the investigation concluded with three packages and three versions of a fourth package being unpublished from the npm Registry.

No packages published to the npm Registry used the malicious modules in a way that would have allowed the backdoor to be triggered. Applications not published to the registry that directly required the malicious modules might have been vulnerable, but are out of the scope of our analysis.

Initial report

Initial information from the community reported that the package `getcookies` contained a potential backdoor, that `express-cookies` and `http-fetch-cookies` depended upon getcookies, and that a popular package, `mailparser`, depended upon http-fetch-cookies.

Source: The npm blog, May 2018

Cryptocurrency startup hacks itself before hacker gets a chance to steal users funds

Backdoor discovered in Agama cryptocurrency wallet. Unconventional tactic saves users from getting robbed.

By Catalin Cimpanu for Zero Day | June 6, 2019 -- 11:05 GMT (19:05 GMT+08:00) | Topic: Security

Source: ZDNet, June 2019

背景： バックドアの脅威
ファームウェア

DEF CON 2019: 35 Bugs in Office Printers Offer Hackers an Open Door

Tara Seals • August 8, 2019 6:00 am

A raft of bugs in six popular models can allow a hacker to wreak havoc on a corporate network.

LAS VEGAS — At least 35 significant vulnerabilities in six commonly used enterprise printers have been uncovered, manufactured by HP, Ricoh, Xerox, Lexmark, Kyocera and Brother.

The bugs will be presented by NCC Group at a DEF CON session entitled "Why You Should Fear Your Mundane Office Equipment" on Saturday. They vary in severity but the potential impact ranges from denial-of-service attacks that could cause the printers to crash, spying on every print job sent and sending print jobs through to unauthorized parties. One of the printers made by HP for instance was affected by multiple overflow vulnerabilities in the Internet Printing Protocol (IPP) service, allowing a potential attacker to effect a denial-of-service (DoS) attack and potentially execute arbitrary code on the device.

Source: ThreatPost

Intel finds critical holes in secret Management Engine hidden in tons of desktop, server chipsets

Bugs can be exploited to extract info, potentially insert rootkits

By Thomas Claburn in San Francisco 20 Nov 2017 at 23:53

Intel today admitted its Management Engine (ME), Server Platform Services (SPS), and Trusted Execution Engine (TXE) are vulnerable to multiple worrying security flaws, based on the findings of external security experts.

The firmware-level bugs allow logged-in administrators, and malicious or hijacked high-privilege processes, to run code beneath the operating system to spy on or meddle with the computer completely out of sight of other users and admins. The holes can also be exploited by network administrators, or people masquerading as admins, to remotely infect machines with spyware and invisible rootkits, potentially.

Source: The Register

背景： バックドアの脅威

IoT 製品

SOHOpelessly Broken 2.0

September 16, 2019

Security Vulnerabilities in Network Accessible Services
Research by: Shaun Mirani, Joshua Meyer, Rick Ramgattie. and Ian Sindermann

Abstract

Internet of Things (IoT) devices have always been vulnerable to a variety of security issues. In 2013, Independent Security Evaluators (ISE) performed research on IoT devices that showed how rich feature sets could be leveraged to compromise devices. Today, we show that security controls put in place by device manufacturers are insufficient against attacks carried out by remote adversaries. This research project aimed to uncover and leverage new techniques to circumvent these new security controls in embedded devices.

Source: www.securityevaluators.com

Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces

(Extended Version)

Andrei Costin
EURECOM
Sophia Antipolis, France
costin@eurecom.fr

Apostolis Zarras
Technical University of Munich
Germany
zarras@sec.in.tum.de

Aurélien Francillon
EURECOM
Sophia Antipolis, France
francill@eurecom.fr

***Abstract*—Embedded devices are becoming more widespread, interconnected, and web-enabled than ever. However, recent studies showed that these devices are far from being secure. Moreover, many embedded systems rely on web interfaces for user interaction or administration. Unfortunately, web security is known to be difficult, and therefore the web interfaces of embedded systems represent a considerable attack surface.**

In this paper, we present the *first fully automated framework* that applies dynamic firmware analysis techniques to achieve, in a scalable manner, automated vulnerability discovery within embedded firmware images. We apply our framework to study the security of embedded web interfaces running in Commercial Off-The-Shelf (COTS) embedded devices, such as routers, DSL/cable modems, VoIP phones, IP/CCTV cameras. We introduce a methodology and implement a scalable framework for discovery of vulnerabilities in embedded web interfaces regardless of the vendor, device, or architecture. To achieve this goal, our framework performs full system emulation to achieve the execution of firmware images in a software-only environment, i.e., without involving any physical embedded devices. Then, we analyze the web interfaces within the firmware using both static

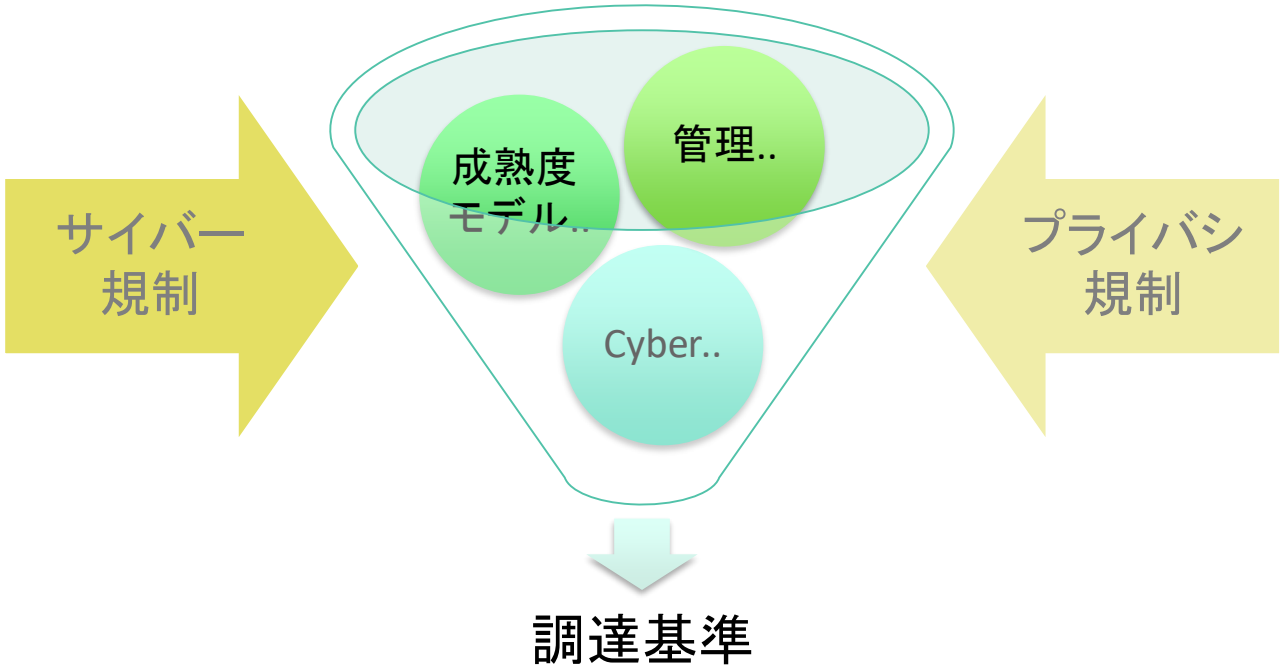
Embedded systems, in particular Small Office/Home Office (SOHO) devices, are often known to be insecure [41,80]. Their lack of security may be the consequence of the harsh market competition. For instance, the time to market is crucial and the competition puts high pressure on the design and production costs, and enforces short release timelines. Vendors try to provide as many features as possible to differentiate products, while customers do not necessarily look for the most secure products.

Some embedded systems have clear and well-defined security goals, such as the pay-TV smart cards and the Hardware Security Modules (HSM). Therefore, such devices are rather secure. However, many embedded systems are not designed with a clear threat model in mind. This gives little motivation to manufacturers to invest time and money in securing them. This fact motivated several researchers to evaluate the state of security of such embedded devices [11,17,24,27,71,79].

Moreover, during the past few years, embedded devices became more connected forming what is called the Internet

Source: BlackHat Asia ‘16

４つの転換点（１）：国際標準から、調達基準へ



国際標準から、調達基準へ：ICSCoE 中核人材育成プログラム2期生の取り組み事例

4

＜電力業界の受講生チーム＞

サプライチェーンセキュリティ研究

Source: ICSCoE Report Vol.05

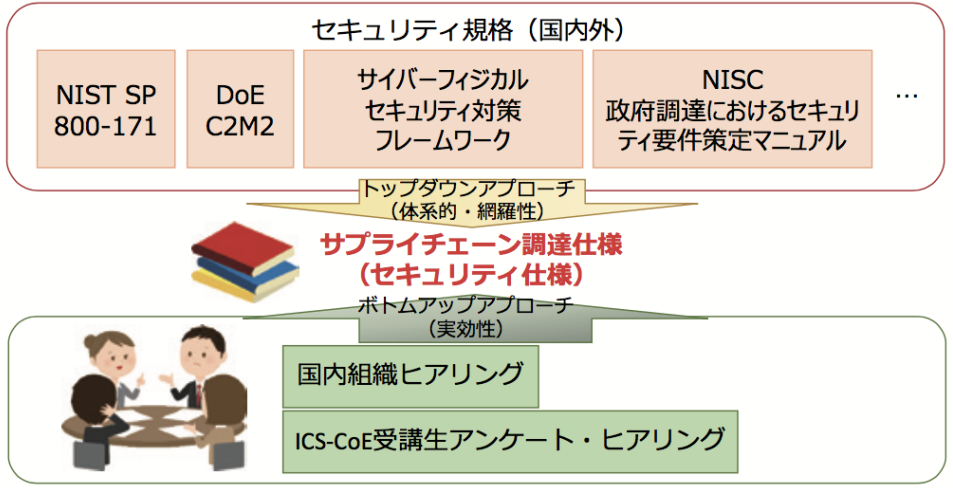
概要

発注から納品までのサプライチェーンにおける不正コード・マルウェア混入を想定したリスクに対処するため、電力業界の受講生を中心に、重要インフラ事業者やベンダ等の受講生とともに、サプライチェーンに特化した調達仕様書を作成しました。

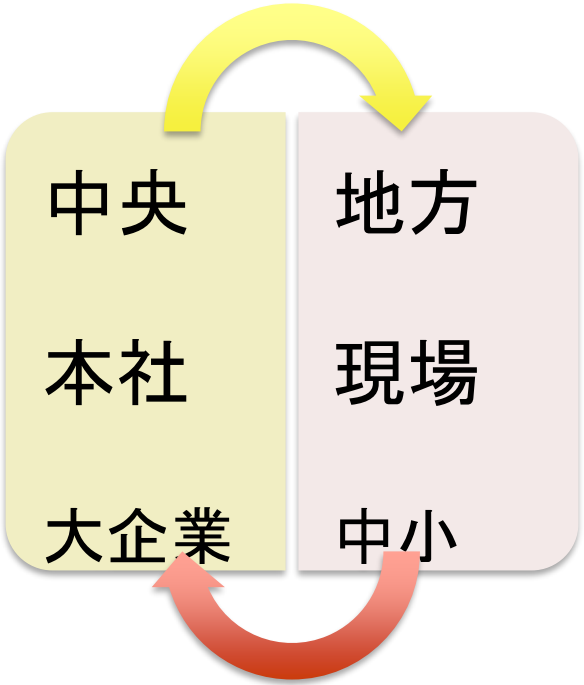
作成にあたっては、国内外のセキュリティ規格をベースにして体系的・網羅的に調達仕様へ反映させていくトップダウンアプローチと、ICSCoE受講生や国内企業へのヒアリングによって調達仕様の実効性を強化するボトムアップアプローチを組み合わせながら進めており、理論だけでなく、実際に使用するところまでを意識した調達仕様書になっていることが大きな特長です。

調達仕様書作成のポイント

✓ 国内外の規格をベースにしたトップダウンアプローチと受講生を中心としたヒアリングによるボトムアップアプローチを組み合わせて実施



４つの転換点（２）：本社の人材育成から、系列・中小企業・現場への波及効果へ



波及効果を目指して:
ICSCoE 中核人材2期生の取り組み事例

<施設管理（ビル）業界の受講生チーム>

施設管理（ビル）業界におけるセキュリティ水準向上を目指して

概要

近年、ビルのシステム運用効率化ニーズやIoT導入を背景として、インターネットを経由したリモート監視や、リモートメンテナンスを実施する例が増えてきています。また、個別の設備システムを統合ネットワークに接続し、機能を連携させる運用なども行われています。このように、ビルを取り巻く環境の変化があることに加え、経済産業省から、ビルシステムのセキュリティ確保を目的としたガイドライン*が公開されるタイミングであったことが活動の契機となり、本プロジェクトを始めました。

*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
https://www.meti.go.jp/press/2019/06/20190617005/20190617005.html

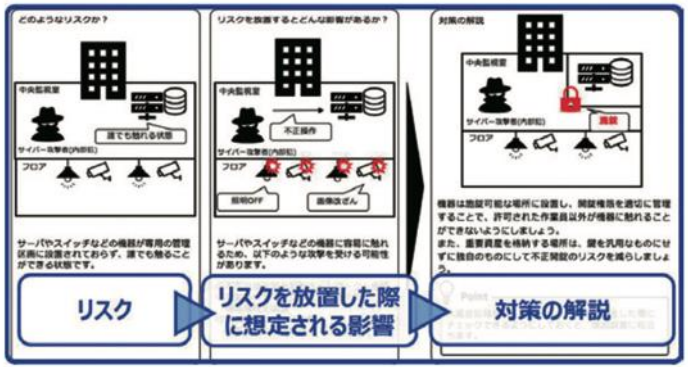
本プロジェクトでは、パブリックコメントの提出を通して、業界の各ステークホルダーがセキュリティのことを自分事として理解されるガイドラインとなるよう、多くの提言を行いました。また、本ガイドラインの業界全体への普及、実践のための理解促進、そして対策推進の第一歩を踏み出す手助けとなることを目的として、ガイドラインの解説書を作成しました。解説書では、独自に以下のコンテンツも提供しています。

① ガイドラインを活用した対策の進め方の提案
② 対策マップ（機器ごとの管理策の対策箇所を可視化）
③ 対策カタログ（リスク／インシデント／対策を図を交えて解説）
④ リスク分析の事例紹介

担当者より

このプロジェクトには、ビルに関わる様々な業界の受講生が集まりましたが、ICSCoEの受講生同士、派遣元企業の枠を超え、フラットな立場で取り組むことができました。解説書はプロジェクトメンバ全員の結束力がなくては完成できなかったですし、ICSCoEにおける1年間の学びの集大成でもあります。業界内で、これからセキュリティに取り組む担当者には、ぜひ読んでいただきたい内容となっています。
ICSCoEで培った知見を活かして、ビル業界におけるサイバーセキュリティ意識の向上と、ステークホルダー間での理解の輪の形成に少しでも貢献できれば嬉しく思います。

解説書（対策カタログ）の構成例



Source: ICSCoE Report Vol.05

本社 (IT)、現場 (OT)

制御システム向けサイバーセキュリティ演習…２日間

本演習では、模擬プロセス制御ネットワークを使用して、機器の不正な制御に使用されるサイバー攻撃や対応策による防御を体験いただきます。制御システムのセキュリティについてより深く理解いただける実践的な内容となっています。

ITと制御システムのアーキテクチャ、セキュリティ脆弱性、および制御システムに固有の対策など、産業用制御システムのセキュリティを習得いただけます。

産業サイバーセキュリティセンター
「製造・生産分野の管理監督者層向けプログラム」

コースについて

1コースは4～5日間。
1コースからでも受講できます。もちろん複数のコースを選択して受講することも可能です。

1. 製造・生産現場のセキュリティに必要なIT・OT基礎

社内の情報システム（IT）部門や制御システム（OT）部門などと連携するうえで必要な知識を学びます。

必須基礎

2. 製造プラント・工場等が稼働している中でのリスク分析手法

製造プラントや工場に対するサイバー攻撃リスクを分析・評価する方法と、製造プラントや工場の稼働を維持した状態でセキュリティを確保するための対策やルール作りに必要な知識を学びます。

現状把握分析

3. 製造・生産現場へのセキュリティ製品導入及びベンダー選定方法

セキュリティ製品やベンダー選定のポイント、セキュリティ要件の作成、要件が正しく実装できているかの確認方法などに必要な知識を学びます。

製品導入

4. 製造・生産現場向けセキュリティ教育の実施方法

現場メンバーとセキュリティを確保するための日常的な取り組みを、QC、カイゼン、KY活動の一部として取り組んでいけるよう指導するために必要な知識を学びます。

現場教育

5. 製造・生産現場でのセキュリティ・インシデント対応実践方法

セキュリティインシデントの可能性も考慮した初動対応、経営層・その他部門との連携に必要な知識、平時からインシデントに備えた対策の策定、再発防止策の作成を学びます。

障害対応

6. 製造・生産現場におけるセキュリティ業務の運用・保守手法

工場やプラント内に設置された機器の資産管理や、導入機器のセキュリティ情報収集、セキュリティ異常に気が付くために必要な知識を学びます。

日常運用

7. 実践 製造・生産現場のためのセキュリティ戦略立案

自社の事業戦略を踏まえ、必要な対策を実現可能な戦略として立案する手法について学びます。

企画・計画

産業サイバーセキュリティセンター
「製造・生産分野の管理監督者層向けプログラム」

■ 参考：企業組織とコースの受講推奨図

A企業の例

スキル＼組織	製造・生産技術管理層				製造・生産現場監督層		
	生産企画	生産技術	工場技術	工場セキュリティ	保全・計装	品証	製造
必須基礎	1. 製造・生産現場のセキュリティに必要なIT・OT基礎						
現状把握分析	2. 製造プラント・工場等が稼働している中でのリスク分析手法						
製品導入	3. 製造・生産現場へのセキュリティ製品導入及びベンダー選定方法						
現場教育			4. 製造・生産現場向けセキュリティ教育の実施方法				
障害対応		5. 製造・生産現場でのセキュリティ・インシデント対応実践方法					
日常運用			6. 製造・生産現場におけるセキュリティ業務の運用・保守手法				
企画・計画	7. 実践 製造・生産現場のためのセキュリティ戦略立案						

B企業の例

スキル＼組織	製造・生産技術管理層			製造・生産現場監督層		
	製造・生産企画	製造・生産技術	工場セキュリティ統括	保全・計装	システム	製造・運転
必須基礎	1. 製造・生産現場のセキュリティに必要なIT・OT基礎					
現状把握分析	2. 製造プラント・工場等が稼働している中でのリスク分析手法					
製品導入		3. 製造・生産現場へのセキュリティ製品導入及びベンダー選定方法				
現場教育			4. 製造・生産現場向けセキュリティ教育の実施方法			
障害対応			5. 製造・生産現場でのセキュリティ・インシデント対応実践方法			
日常運用			6. 製造・生産現場におけるセキュリティ業務の運用・保守手法			
企画・計画	7. 実践 製造・生産現場のためのセキュリティ戦略立案					

：推奨講座　　：受講が望ましい

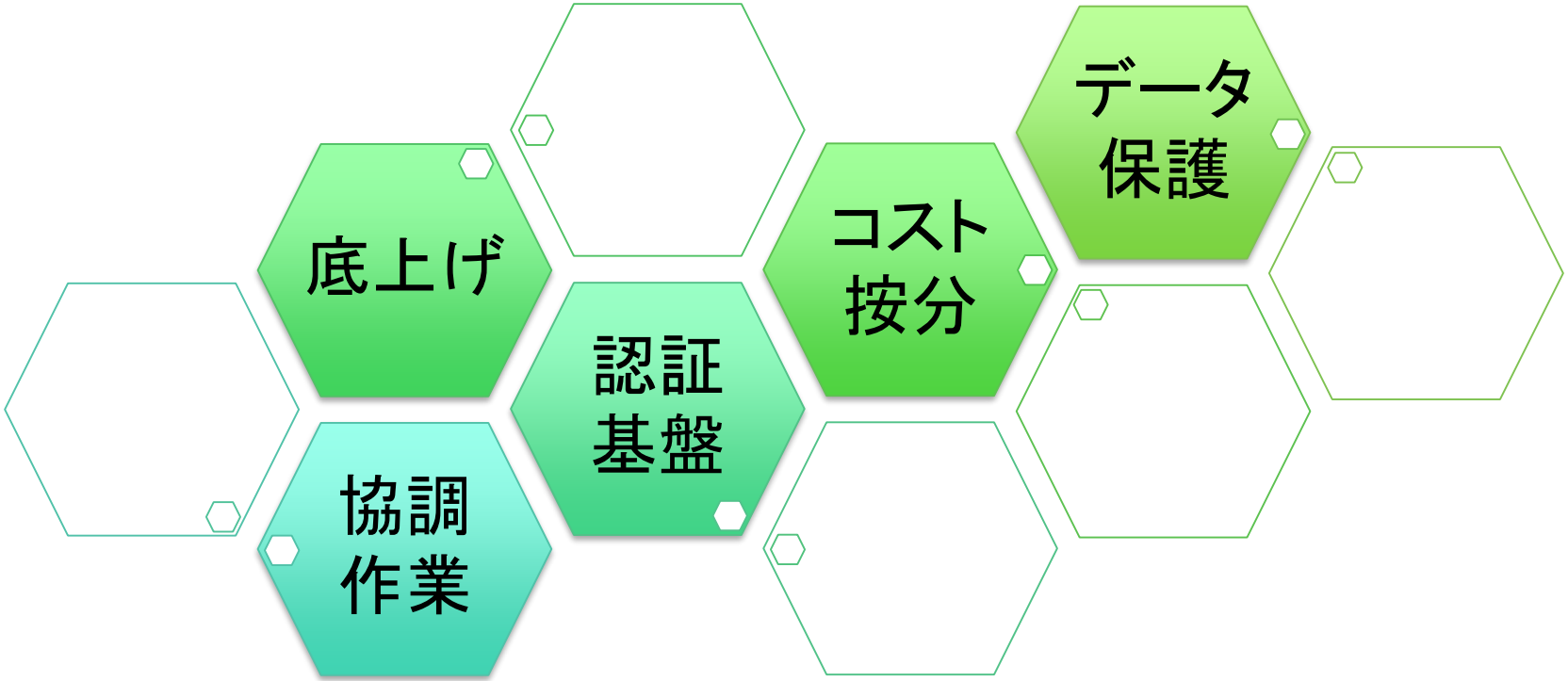
業界別サイバーレジリエンス強化演習（CyberREX（サイバーレックス））…２日間

本演習は、部署・部門のサイバーセキュリティに関する対応力・回復力の強化、業界特性を意識した企業組織全体の強靭化を目的としています。
業界別に仮想企業を想定した、シナリオによる実践的演習の形式を中心としたトレーニングとなっていることが特徴です。また、海外子会社、系列企業、サプライチェーン等のビジネスパートナーが直面するサイバーセキュリティ規制やガイドライン等の解説に関する集中講義を行います。

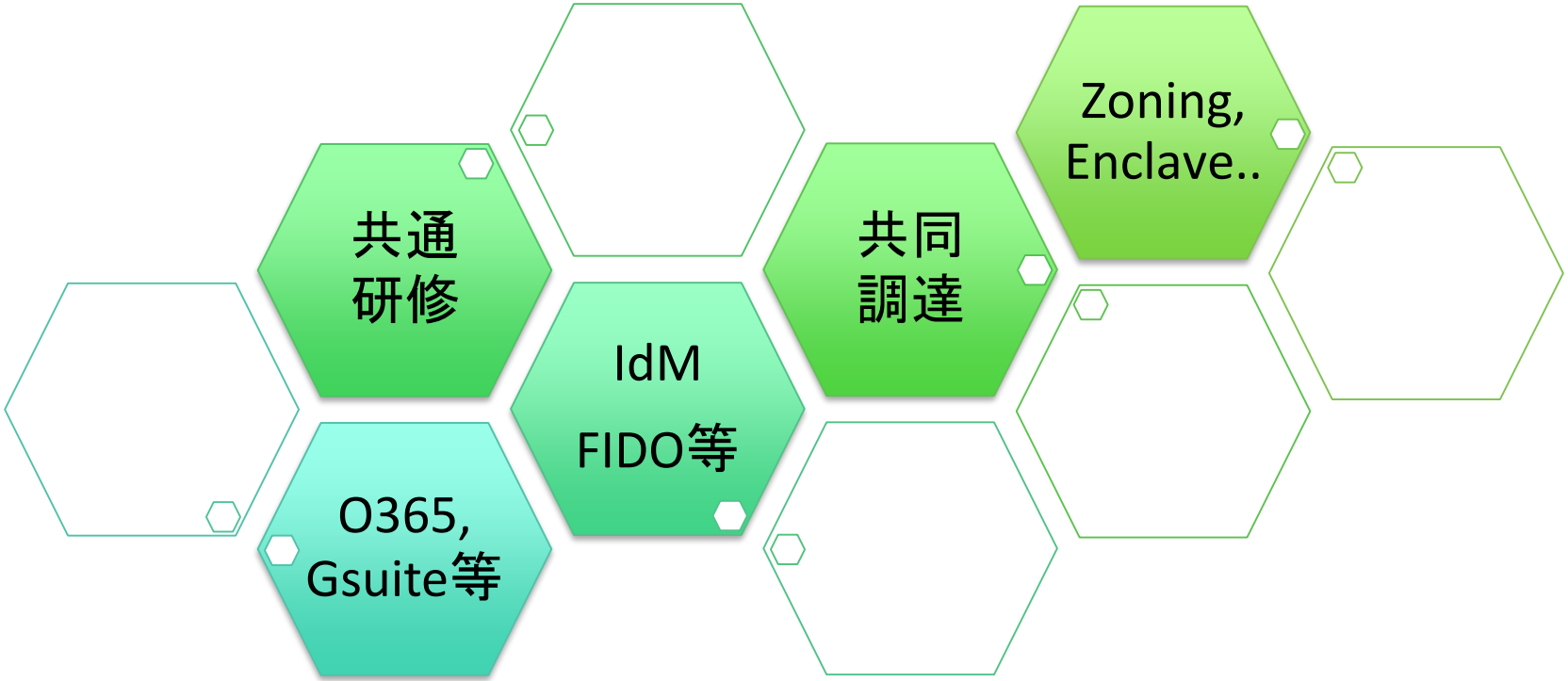
サイバー危機対応机上演習（旧・国際トレーニング）…２日間

本演習では、高度なサイバー脅威が増加していることから、制御システムを有する企業を守るベストな方法とは何か、そして自社組織に適用可能なサイバーセキュリティ投資の根拠となるリスク分析、インシデント管理の実行フレームワークについての講義及び机上演習を行います。
机上演習は、米国サイバー軍出身者らによるウォーゲーム形式で、「CISO」「工場長」「広報担当者」などの役割を体験しつつ、企業を守るスキルとメソッドを習得します。

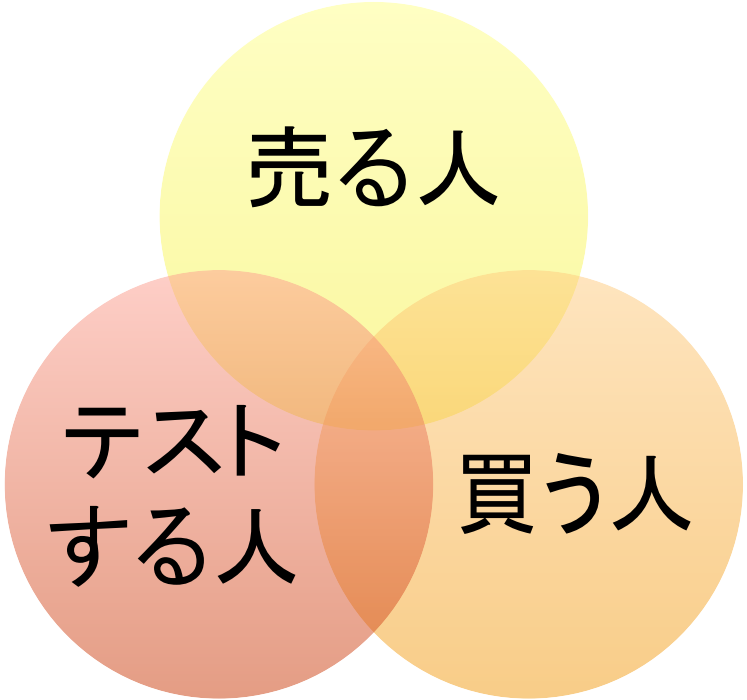
４つの転換点（３）：
自社でのクラウド活用から、経済圏でのクラウド活用へ



自社でのクラウド活用から、経済圏でのクラウド活用へ



４つの転換点（４）：
「よろしく」から、Trust but Verify へ



FTC vs D-Link 判決で求められている項目（一部）

FEDERAL TRADE COMMISSION v. D-LINK SYSTEMS, INC., Case No. 3:17-cv-00039-JD.

- Security planning
- Threat modeling
- Pre-release code review
- Pre-release vulnerability testing
- Ongoing code maintenance
- Remediation processes for software flaws
- Ongoing monitoring of security research
- A process for accepting vulnerability reports
- Automatic firmware updates
- Biennial security training

まとめ

4つの転換点
1. 国際標準から、調達基準へ
2. 本社の人材育成から、中小企業・現場への波及効果へ
3. 自社でのクラウド活用から、経済圏でのクラウド活用へ
4.「よろしく」から、Trust but Verify へ

先進例 – 産業サイバーセキュリティセンターの取り組みから

「サプライチェーンセキュリティ向上 ＝ 経済圏のセキュリティ向上」