

制御システムセキュリティの 重要性

一般社団法人JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
落合 一郎

目次

- 制御システムアセットオーナーの調査結果
 - 2015年の調査結果と2013年からの経年変化
 - 制御システムセキュリティ対策の重要性理解の状況
- 必要とされる制御システムセキュリティ対策
 - 対策の両輪
 - ICS-CERT推奨技術戦略
- まとめ

2015年の途中集計結果と2013年からの経年変化

制御システムアセットオーナー 調査結果

調査（アンケート）の目的と内容

2015年末に2013年とほぼ
同じ項目で実施しました

■ 目的

- 制御システム使用状況の把握
- セキュリティリスクの認識と対策状況の把握

■ 主な内容

- マルウェア感染有無
- PLC, SCADA, DCSの使用有無
- ネットワーク接続状況
- 制御システムセキュリティ対策実施状況
- 制御システムセキュリティ情報の入手状況
- セキュリティリスクの評価実施状況
- インシデント発生可能性の認識
- 事故が起こったときの頼り先
- インシデントが発生した場合に備えた体制有無
- 今後の制御システムセキュリティ対策方向性

調査対象：多業種

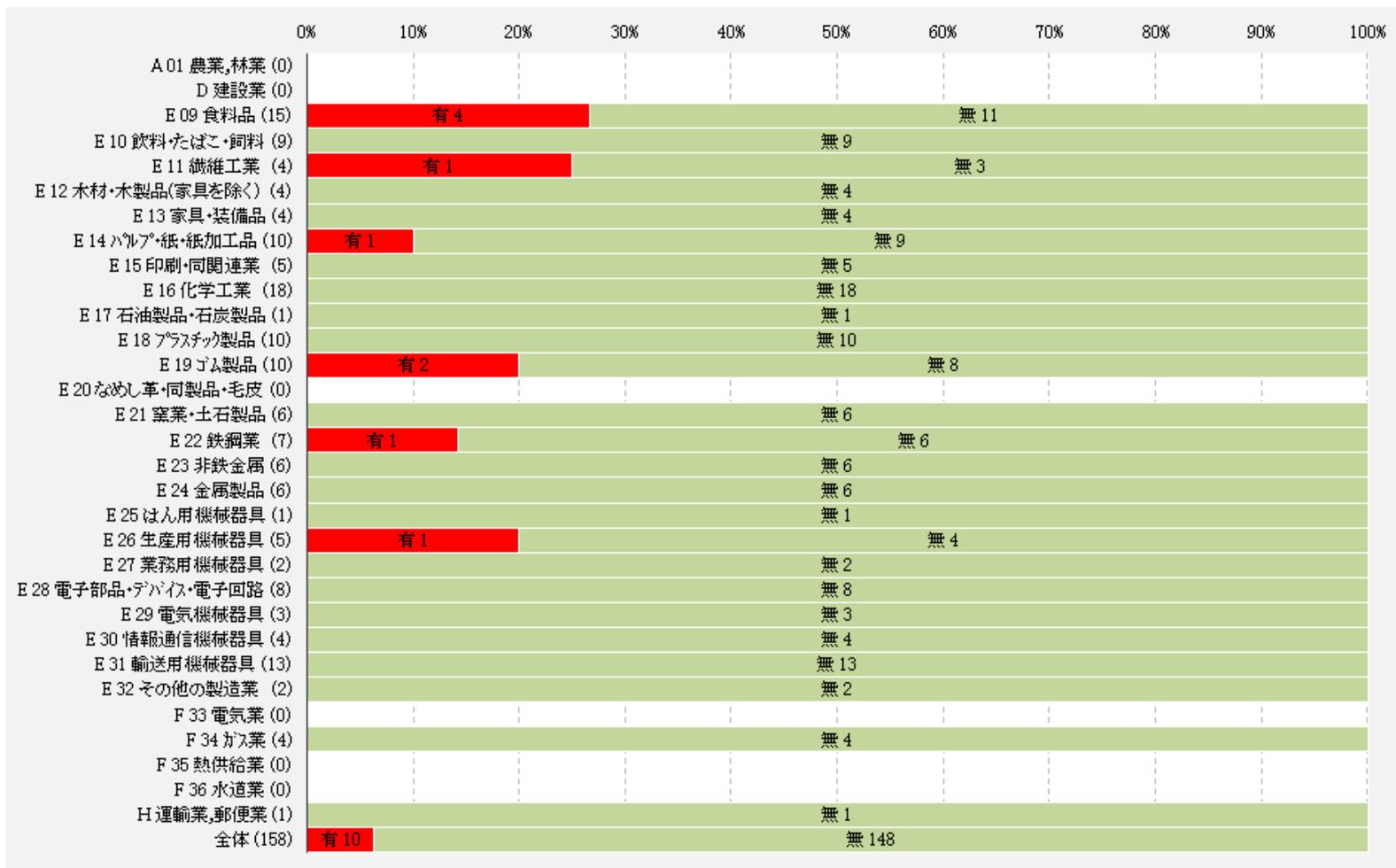
	業種大分類	2013	2015
A 01 農業, 林業	A 01 農業, 林業		
D 建設業	D 建設業		
E 製造業	E 09 食料品製造業	15	15
	E 10 飲料・たばこ・飼料製造業	9	9
	E 11 繊維工業	12	4
	E 12 木材・木製品製造業(家具を除く)	3	4
	E 13 家具・装備品製造業	3	4
	E 14 パルプ・紙・紙加工品製造業	12	10
	E 15 印刷・同関連業	19	5
	E 16 化学工業	20	18
	E 17 石油製品・石炭製品製造業	5	1
	E 18 プラスチック製品製造業(別掲を除く)	11	10
	E 19 ゴム製品製造業	11	10
	E 20 なめし革・同製品・毛皮製造業		0
	E 21 窯業・土石製品製造業	11	6
	E 22 鉄鋼業	13	7
	E 23 非鉄金属製造業	11	6
	E 24 金属製品製造業	14	6
	E 25 はん用機械器具製造業	11	1
	E 26 生産用機械器具製造業	11	5
	E 27 業務用機械器具製造業	11	2
	E 28 電子部品・デバイス・電子回路製造業	17	8
E 29 電気機械器具製造業	13	3	
E 30 情報通信機械器具製造業	9	4	
E 31 輸送用機械器具製造業	25	13	
E 32 その他の製造業	7	2	
F 電気・ガス・熱供給・水道業	F 33 電気業		0
	F 34 ガス業	4	4
	F 35 熱供給業		0
	F 36 水道業	23	0
H 運輸業, 郵便業	H 運輸業, 郵便業		1
全体	全体	300	158

最終的には300社以上の予定
今回は途中集計データです

マルウェアの感染は起こっている

■ マルウェア感染数

—2015年：10社/158社=6.3% ← 2013年：22社/300社=7.3%



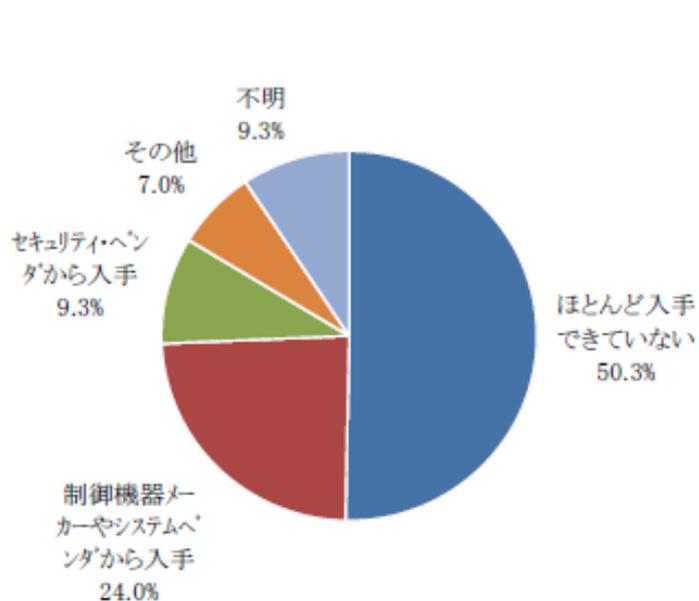
マルウェア感染はUSBメモリから

- 2015年では半日程度の操業停止が1件報告されている
- 判明している感染経路はやはりUSBメモリが多い
- 期間を指定していないので、過去に感染があったもの

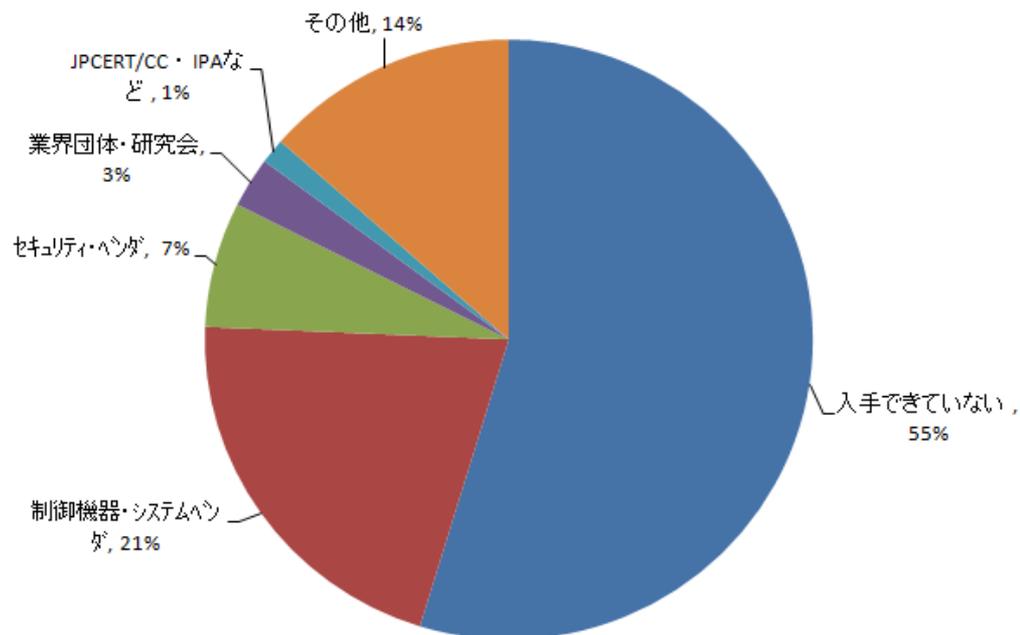
業種分類	時期	内容	被害内容	システムダウン	
				期間	被害額
E 09 食品製造業	2年以上前	USB フラッシュドライブ経由のマルウェア	その他（被害を受ける前に対応できた。）		
E 09 食品製造業	2年以上前	USB フラッシュドライブ経由のマルウェア	その他（被害を受ける前に対応した。）		
E 09 食品製造業	2年位前	詳細不明	その他（被害を受ける前に駆除した。）		
E 11 繊維工業	1年以内	詳細不明	その他（感染したが、被害は無かった。）		
E 14 パルプ・紙・紙加工品製造業	2011～2012年頃	詳細不明	操業停止	半日程度	不明
E 19 ゴム製品製造業	2年以上前	詳細不明	その他（システムが不安定になった。）		
E 09 食品製造業	3～4年前	トロイ	その他（確認できたので駆除した。）		
E 22 鉄鋼業	2012～2013年頃	詳細不明	その他（感染したとすぐに分かったので、何も被害は無かった。）		
E 26 生産用機械器具製造業	5～6年くらい	詳細不明	その他（装置の速度が少し遅くなった。）	数時間	不明
E 19 ゴム製品製造業	1～2年前	詳細不明	その他（データベースが見られなくなったが、担当者が対応して復旧した。）		

セキュリティ情報は入手できていない

i. 入手しているICS製品のセキュリティ情報



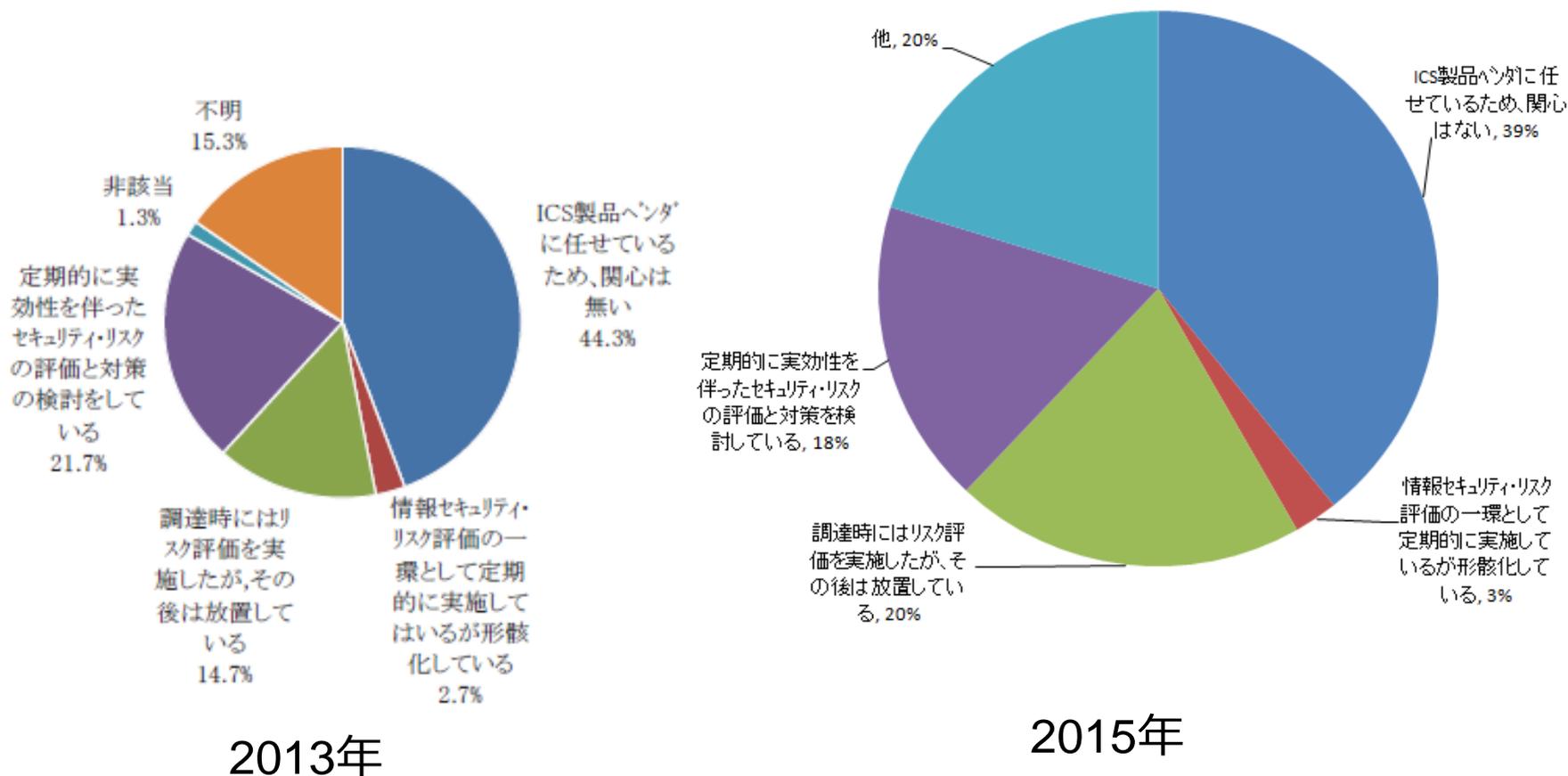
2013年



2015年

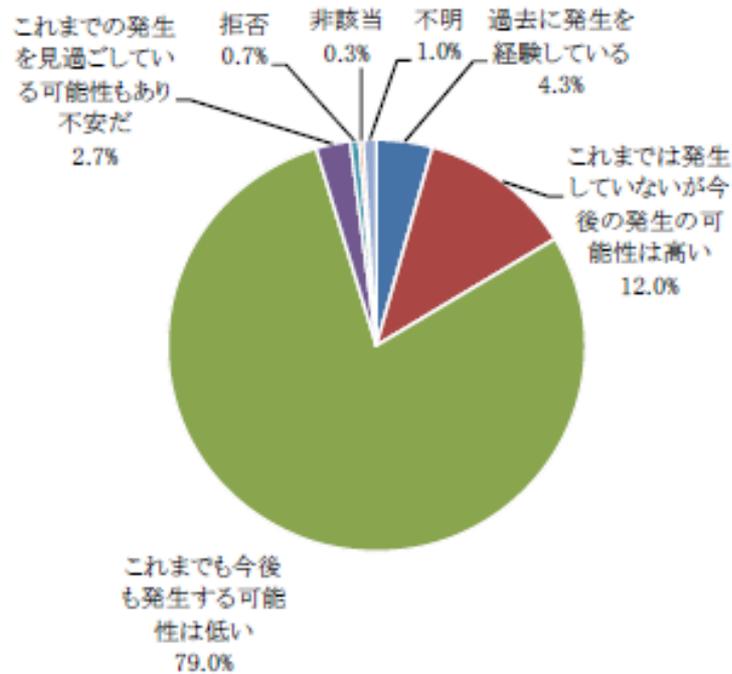
セキュリティリスクは評価されていない

ii. ICSのセキュリティ・リスクに関する評価

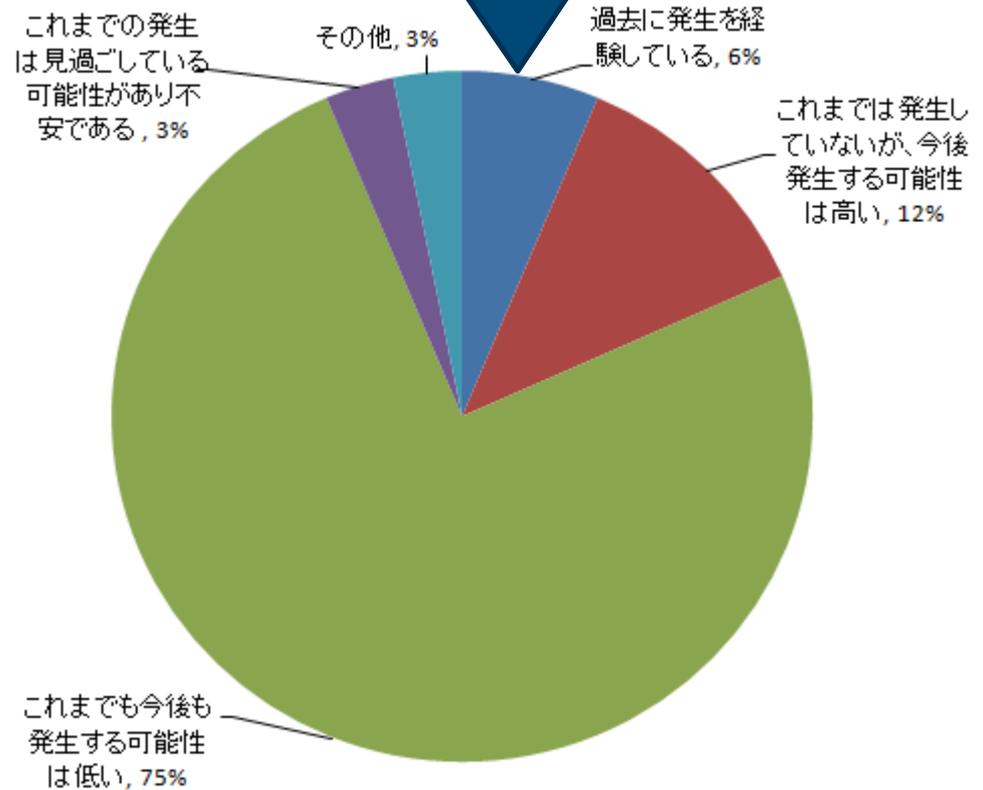


インシデントは発生しないと思われる

iv. ICSのセキュリティ・インシデント発生の可能性に対する認識



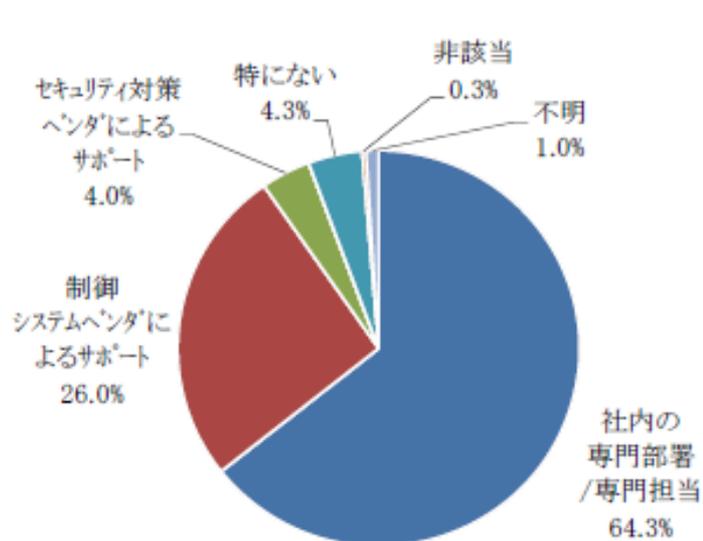
2013年



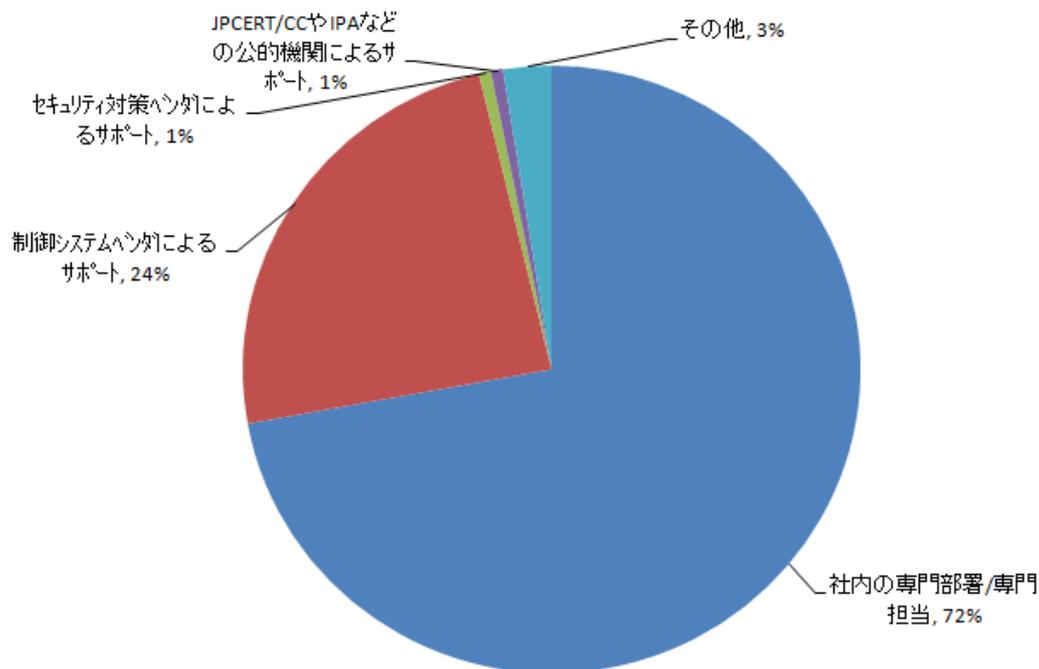
2015年

事故発生時に頼るのは社内専門家かベンダー

v. 万一にもセキュリティ事故が起きた時の頼り先



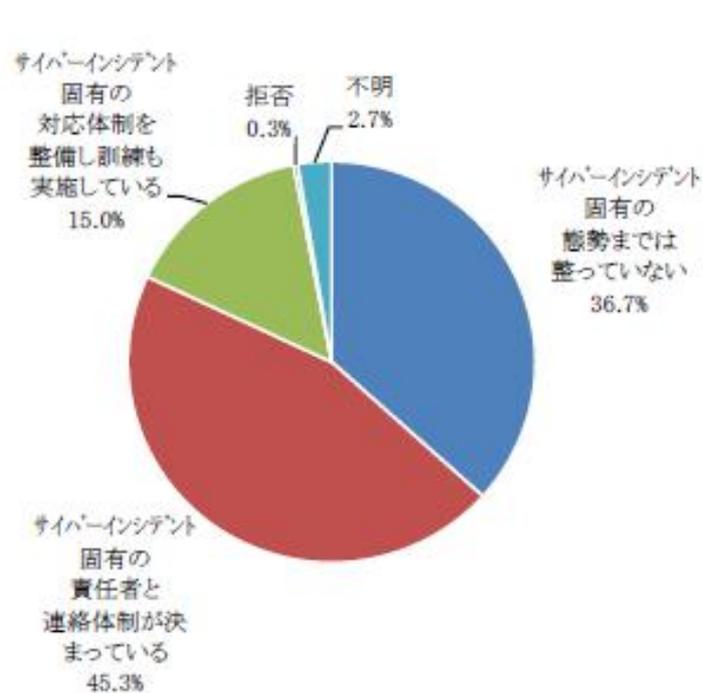
2013年



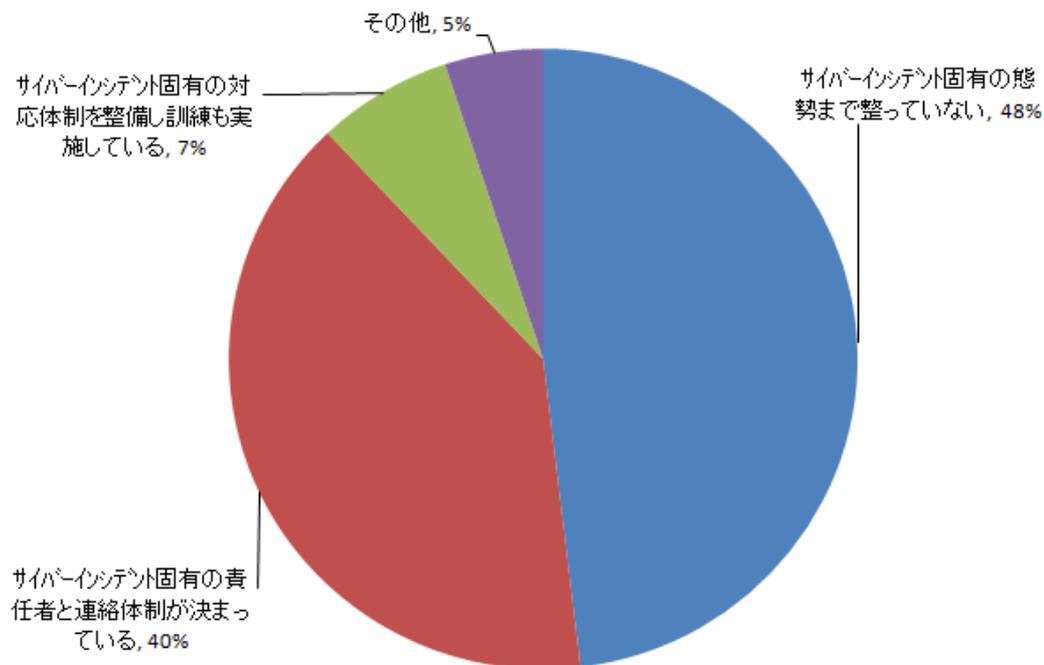
2015年

インシデント対応態勢はできていない

vii. ICSのセキュリティ・インシデントが発生した場合に備えた態勢が整っているか。



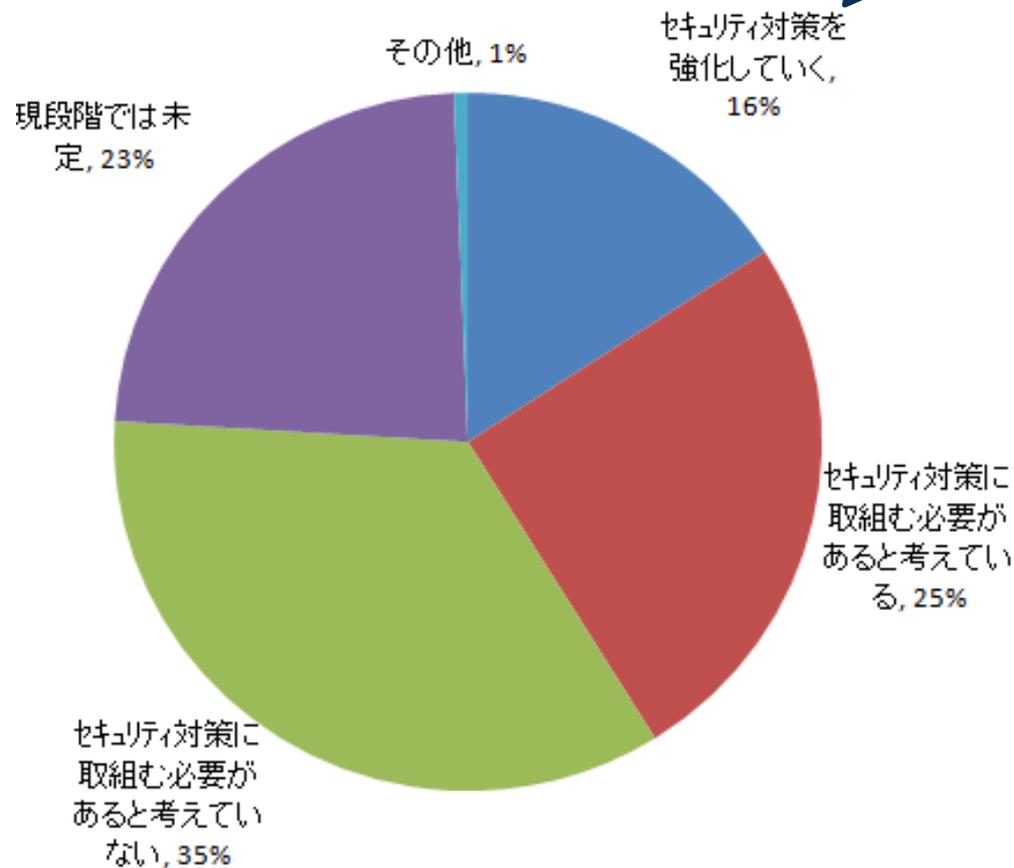
2013年



2015年

今後のセキュリティ対策の方向性は2分化

現状で対策されている割合



2015年

まとめ：それでも、セキュリティ対策は重要

アンケートから読み取れること

- ★セキュリティ情報を入手していない。
- ★セキュリティリスクを評価できていない。
- ★インシデントは発生しないと考えている。
- ★社内の担当者が解決しようとしているが…。

海外

国内

- 今は、運良くあまりウイルス感染などのインシデントが発生していない
- オフィス環境を狙ったウイルスが侵入しても影響は小さい

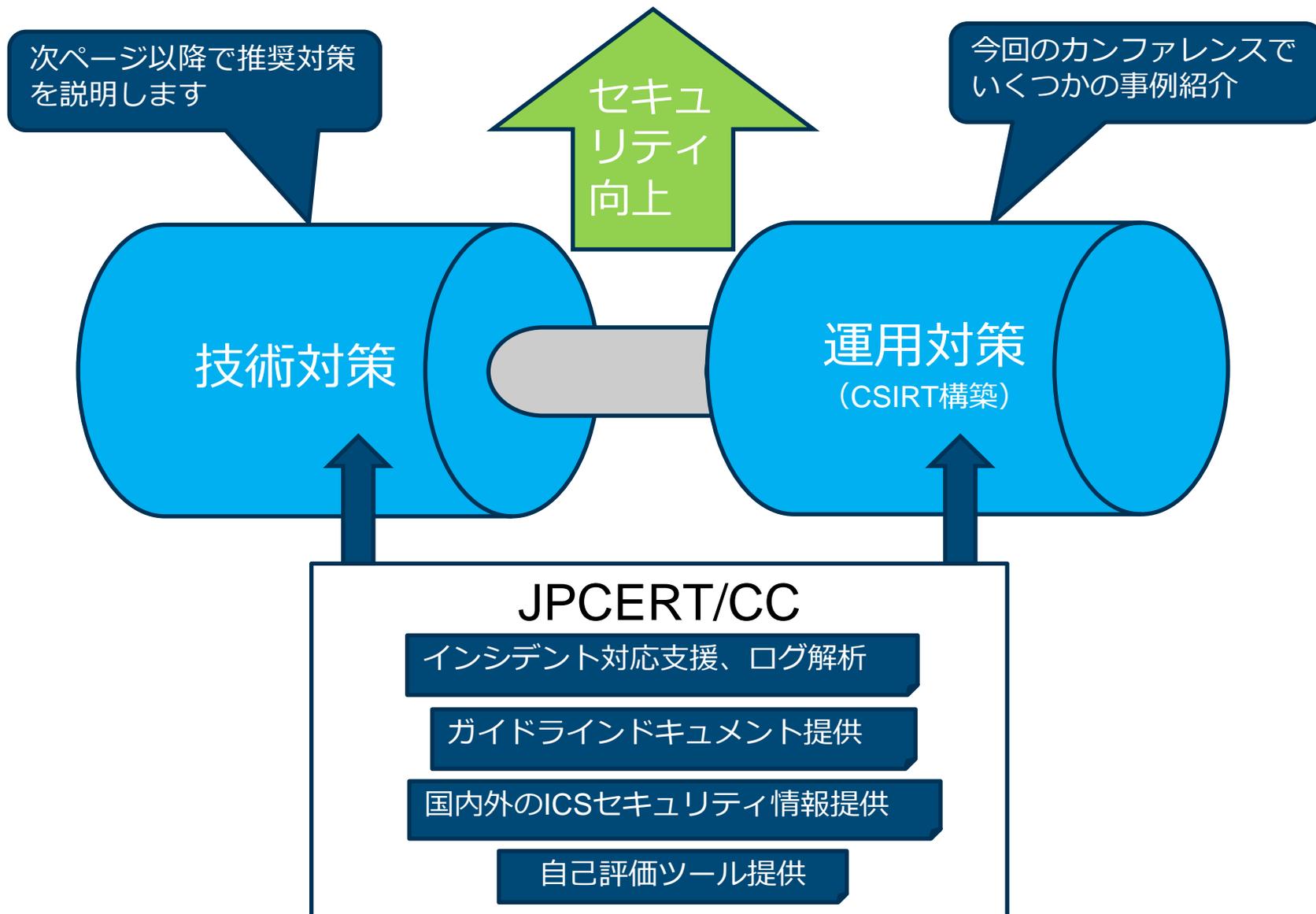
ウクライナの大規模停電
ドイツの製鉄所の事故
ダイムラークライスラー
の事故

国内は依然セキュリティ対策は進んでいないことが明らかになったが、インシデント発生可能性は大きくなりつつあり、一旦発生してしまえば、大きな被害になる

セキュリティ対策は重要

必要とされる 制御システムセキュリティ対策

セキュリティ対策の両輪

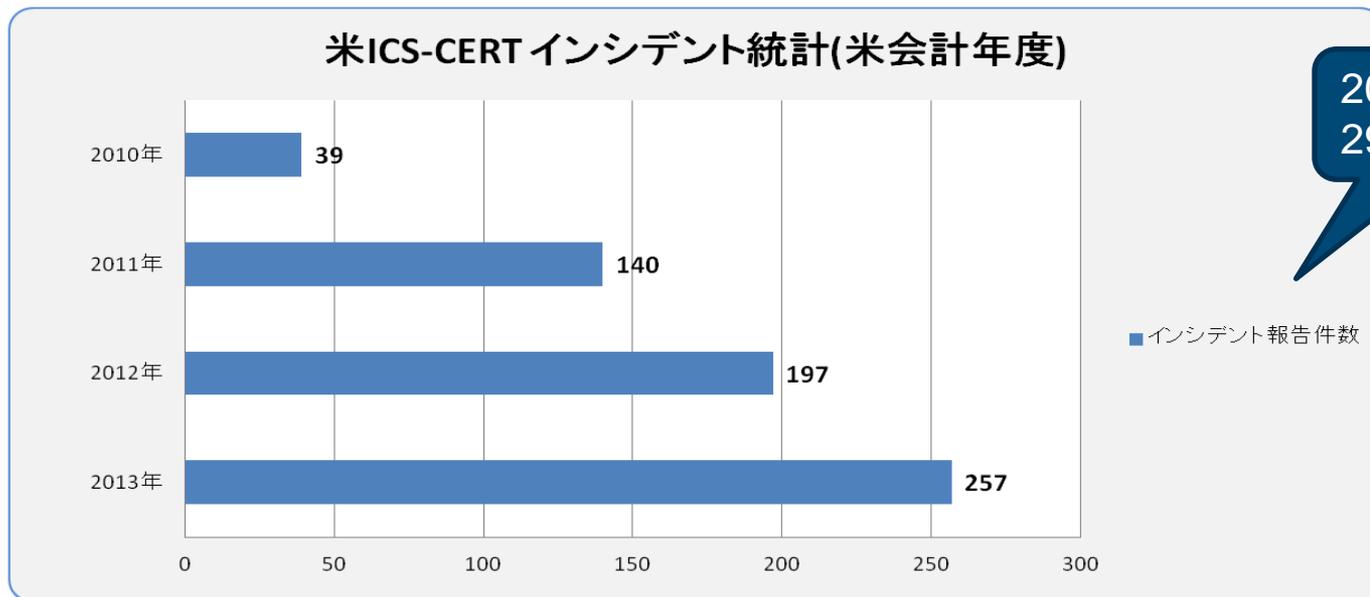


ICS-CERTとインシデント対応状況

■ ICS-CERTとは

- ICS（制御システム）専門のCERT組織
- 米国DHS内の組織
- インシデント対応、脆弱性ハンドリング、アセスメント、ガイドドキュメント公開

■ ICS-CERTインシデント報告件数



ICS-CERT推奨技術戦略



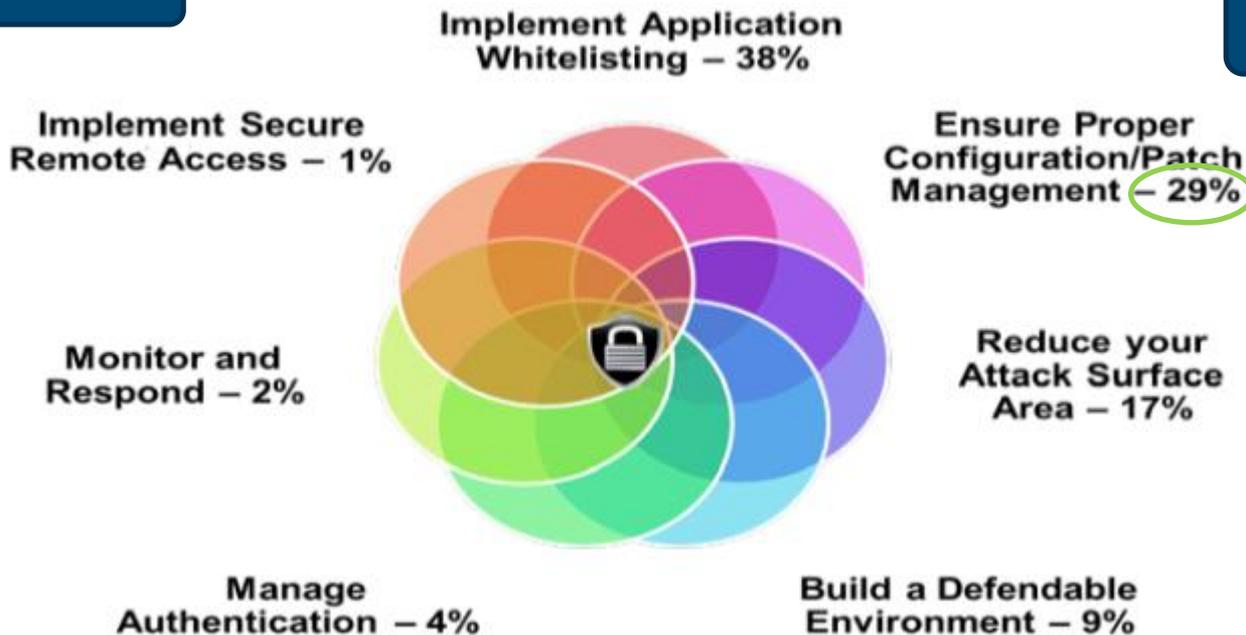
この3組織が協力して作成

7つの戦略

—これらの戦略が実現されていけば2014, 2015年度に報告されたインシデントの98%を阻止できたであろうと述べています。

500件程度

Seven Strategies to Defend ICSs



この戦略によって阻止できた割合

<https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems>

Implement Application Whitelisting

ホワイトリストの導入

- Whitelist ⇔ Blacklist (Anti-Virus)
- ICS環境に適している
 - ICS環境では稼働後の変更が少ない
 - パターンファイルの更新が必要ない
 - 古いOSにも適用できる
 - 未知のマルウェアからの保護も可能
- ソフト選択、導入時に検討すべきこと
 - ホワイトリストの種類
 - ファイルPath, ファイル名, ファイルサイズ, シグネチャ, ...
 - 動作モード
 - 制限、モニタリング
 - ウイルスチェック後に導入
- ガイドドキュメント：NIST 800-167

一般オフィス環境
への導入には課題
が多い

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf>

Ensure Proper Configuration/Patch Management

パッチ管理と設定変更管理

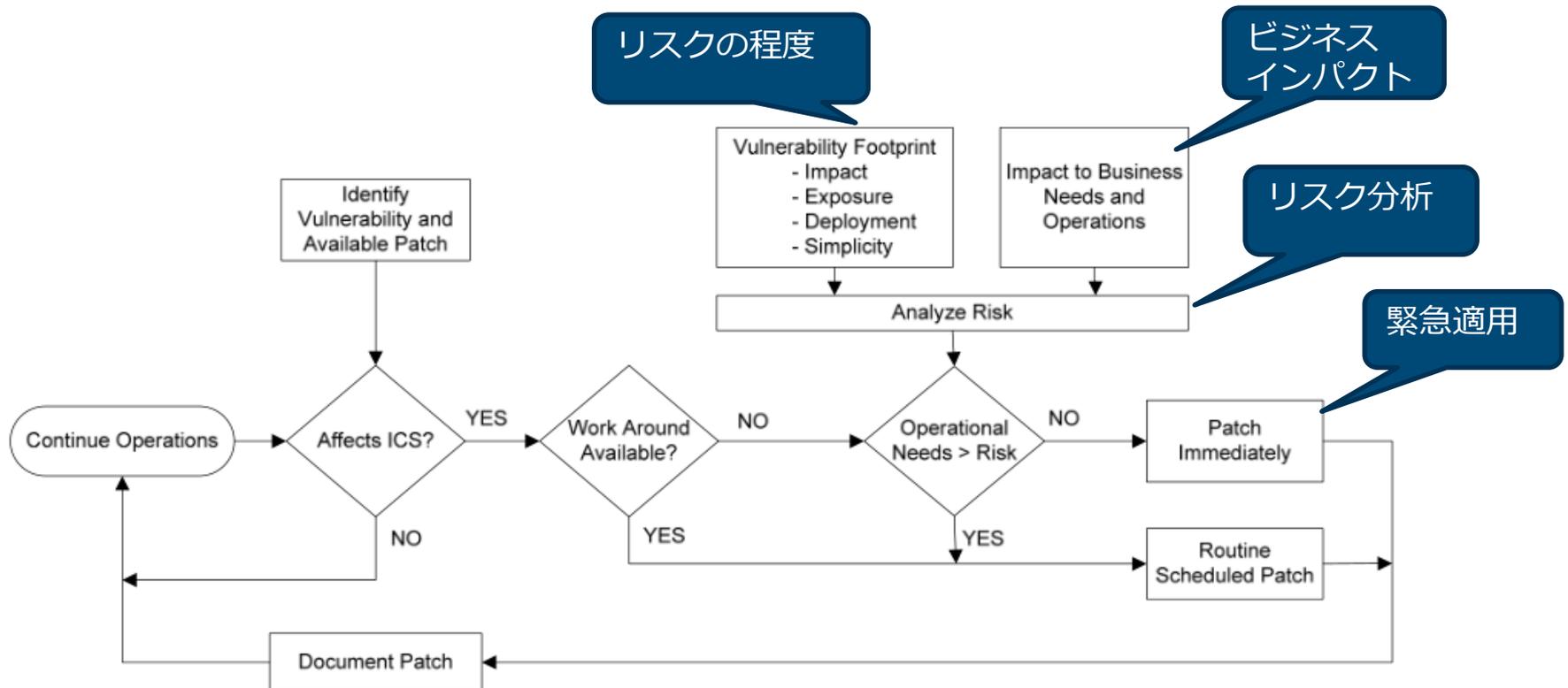
- 攻撃者はパッチのあたっていないシステムを狙う
- 正規のパッチを取得する
 - Havexは改ざんされたパッチで拡散
- 機器の棚卸→必要なパッチの確認

Ensure Proper Configuration/Patch Management パッチ管理と設定変更管理

■ ガイドドキュメント

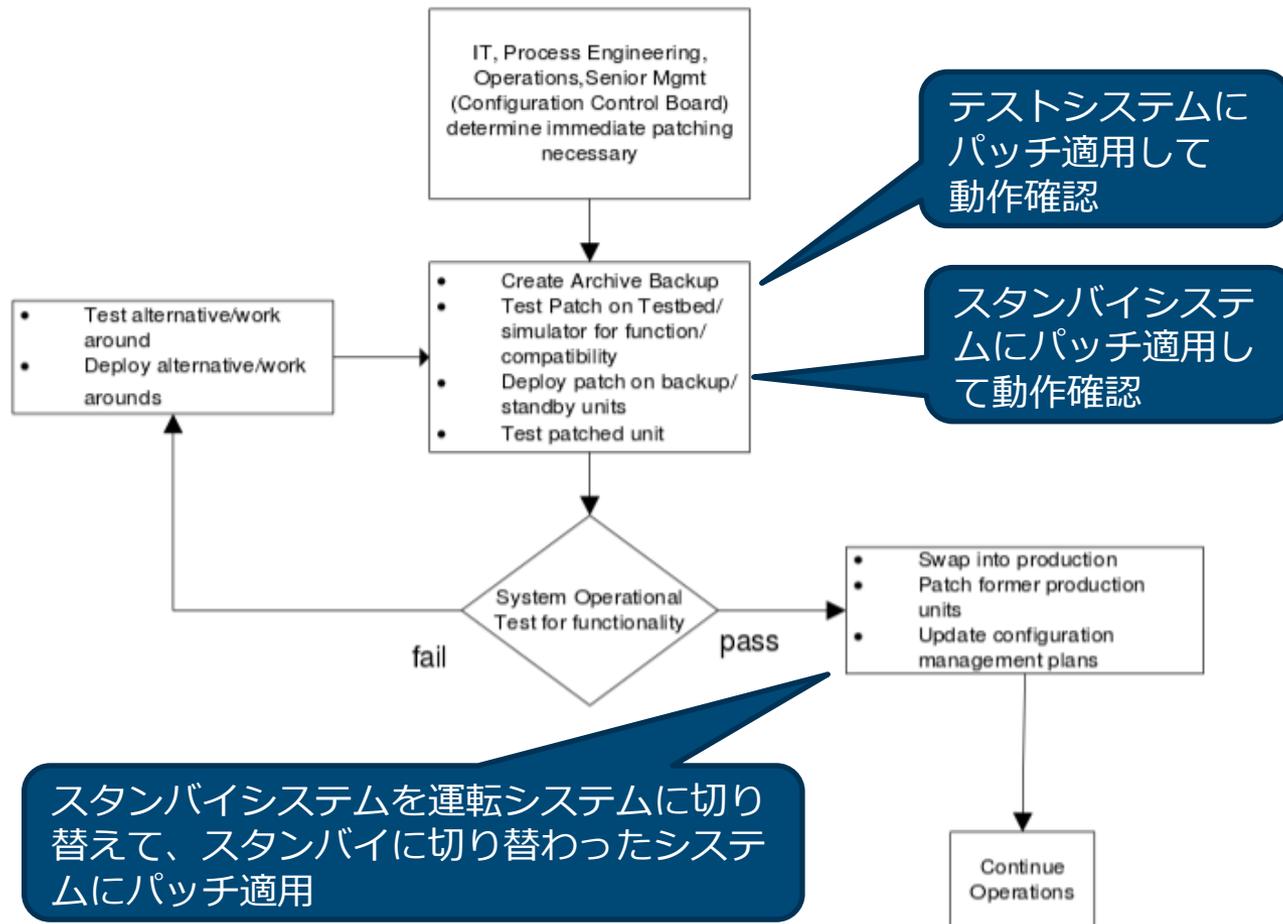
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

■ セキュリティパッチ緊急適用判断フローチャート



Ensure Proper Configuration/Patch Management 適正なパッチ管理と設定変更管理

■ パッチ適用手順



Reduce your Attack Surface Area 攻撃の侵入口を減らす

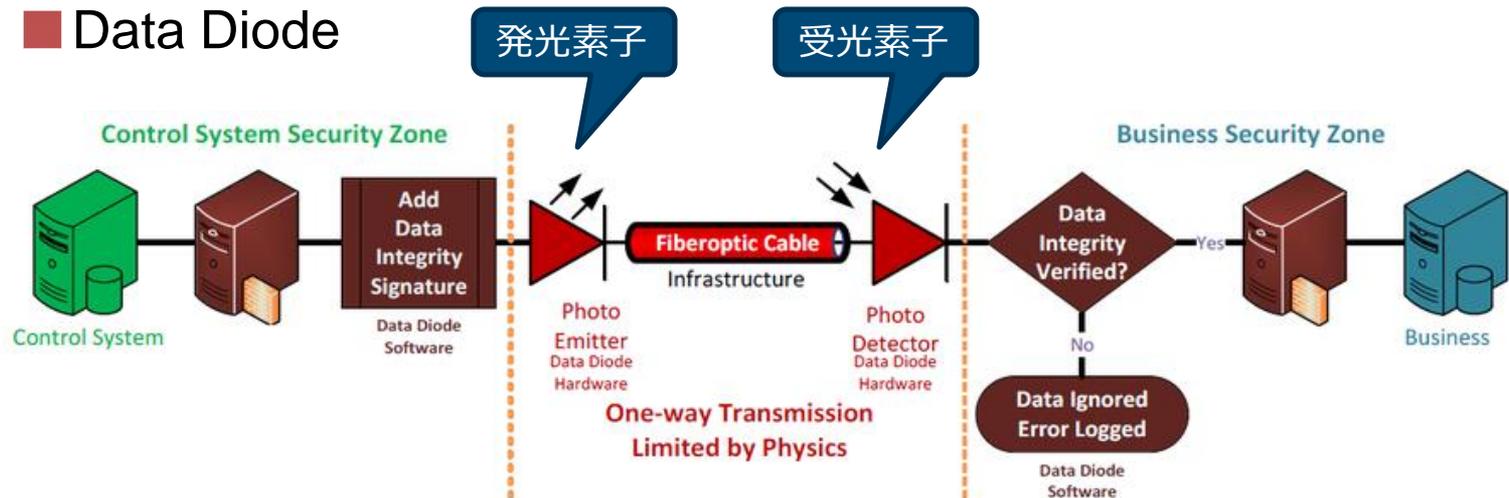
■ ネットワーク隔離

特にインターネット
接続に注意

■ ハードニング

- 未使用ポートの無効化
- 未使用サービスの無効化
- 外部ネットワーク接続の適正設定

■ Data Diode



<https://techsupport.osisoft.com/Troubleshooting/KB/KB01099>

Build a Defendable Environment

防御しやすい環境を作る

- セグメント分け、または、ゾーニング
 - 論理的なつながりで、ネットワークを分離
- 効果・目的
 - 攻撃者がほかのセグメント（ゾーン）にアクセスできないようにする
 - マルウェア感染の範囲を限定
 - インシデント対応の「封じ込め」にも有効

Manage Authentication 認証管理

- 攻撃者は認証情報、特に特権アカウントを狙うケースが増えている
 - 特権アカウントが奪われると、ユーザのなりすまし、証拠の隠滅などが行われる
 - パスワードの厳重管理、マルチファクタ認証
- コーポレートのIDとICS環境のIDは分けて管理する
 - AD等の共有は絶対しない

Implement Secure Remote Access

安全なリモートアクセスを導入

- モデムは仕組み的にセキュリティが考慮されていない
- オペレータによる意図したバックドアに注意
- 可能な限り「監視のみ」に設定する
- ベンダーの常時リモート接続は許可しない
- リモートアクセスはオペレータによる管理のもと、制限時間のある接続に限ること
- 可能であればマルチファクタ認証とし、鍵は厳密に管理する

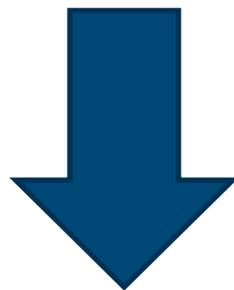
Monitor and Respond モニタリングと対応

- 近年の脅威に対応するためには、**侵入検知**と準備された迅速な対応が重要
- モニタリングポイント
 - ICSの境界におけるIPトラフィック
 - 制御ネットワーク内のIPトラフィック
 - マルウェアによる通信
 - AVソフトによる検出
 - ログイン情報の解析
 - アカウント情報変更の監視
- 攻撃が検出されたときの対応計画を**事前**に用意すること

まとめ

まとめ

- 日本国内においては2015年の調査においても2013年と比較して状況は改善しているようには見えない
- 制御システムセキュリティの重要性はますます高まっている
- ICS環境への技術対策が体系的に説明されたレポートが公開された



2016年はICSセキュリティ対策の強化を期待

JPCERTの提供サービス

トップページ

情報提供

- ・ 注意喚起
- ・ 早期警戒
- ・ 脆弱性対策情報
- ・ Weekly Report
- ・ インターネット定点観測

インシデントの報告

各種登録

制御システムセキュリティ

- ・ 制御システムセキュリティとは
- ・ インシデント報告

ラーニング

公開資料

イベント

プレスリリース

JPCERT/CC

公募・入札情報

関連組織



制御システムセキュリティとは

制御システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学システムの監視制御など国民生活の基盤サービスを提供する重要なシステムとして利用されてきた。近年、サイバー攻撃の増加に伴って脆弱性が発見されるという事案も散見され始めています。JPCERT/CCでは、プロセス監視調整機関として対策の促進に資する活動を進めています。

- ・ 制御システムインシデントの報告
- ・ 制御システムセキュリティに関する情報提供
- ・ ガイドライン、参考資料
 - ・ 制御システムセキュリティプロトコル
 - ・ 制御システムセキュリティガイドライン(全)
 - ・ 分野別セキュリティ規準及びガイドライン
 - ・ セキュリティマネジメント全般
 - ・ 参考資料「制御システム用製品の開発ベ

資料

- ・ SHODANを悪用した攻撃に備えてー 制御システムセキュリティ
- ・ 制御システムセキュリティガイドライン、標準
- ・ 「制御系プロトコルに関する調査研究」報告書
- ・ 国内の制御システム、制御系プロトコルに

関連ツール

- ・ 日本版SSAT(SCADA Self Assessment Tool)
- ・ 制御システムセキュリティ自己評価ツール

アカウント情報 | ログアウト

JPCERT/CC®

ホーム | お問い合わせ | ConPaSについて

MENU

- ▽ 制御システムセキュリティ情報
 - ニュースクリップ
 - ニュースレター
 - 参考情報
 - ICS-CERT公開情報
- ▽ 制御システムセキュア化ガイド集
 - セキュリティシステムの構築/概要
 - セキュリティ管理システムの評価
 - セキュリティの強化対策
 - インシデント事前/事後対応
- ▽ 調査・研究報告書
 - JPCERT/CC
 - 外部組織
- ▽ イベント情報
 - イベントスケジュール
 - 講演資料

新着情報

検索

制御システムセキュリティ情報

ニュースクリップ 2016	2016/01/28
ICSA-16-026-01 : MICROSYS の PROMOTIC にメモリ破壊の脆弱性	2016/01/27
ICSA-16-026-02 : Rockwell Automation の MicroLogix 1100 PLC にスタックベースバッファオーバーフローの脆弱性	2016/01/27
ニュースクリップ 2015	2016/01/25
ICSA-15-337-02: Hospira の複数製品にバッファオーバーフローの脆弱性	2016/01/25

もっと見る

その他

[制御システムセキュア化ガイド集]	2015/07/22
NIST SP 800-82 産業用制御システム(ICS)のセキュリティガイド	
[調査・研究報告書] ICS-CERT モニター (2015年5月~6月)	2015/07/08

お問合せ、ご相談は

Home

サイト内検索

検索

トップページ

情報提供

- 注意喚起
- 早期警戒
- 脆弱性対策情報
- Weekly Report

各種届出・申込

- 制御システムセキュリティ
- ラーニング
- 公開資料

- 四半期レポート
- 研究・調査レポート
- CSIRTマテリアル

イベント

- プレスリリース
- JPCERT/CC

JPCERTコーディネーションセンター 制御システムセキュリティ対策グループ

制御システムセキュリティに関するご相談

— Email : icsr@jpcert.or.jp

— <https://www.jpcert.or.jp/ics/>

制御システムインシデントの報告

— Email : icsr-ir@jpcert.or.jp

— <https://www.jpcert.or.jp/ics/ics-form>

御静聴ありがとうございました