

制御システムセキュリティへの取組み



2016年2月17日

住友化学株式会社

目次

1. 会社概要
2. 制御システムセキュリティ対策の背景
3. 制御システムセキュリティ対策の経緯
4. 制御システムセキュリティの特徴
5. 問題意識・課題と対応
 - 5.1 問題意識・課題
 - 5.2 問題意識・課題への対応
 - 5.3 問題意識・課題への対応まとめ
6. 制御システムセキュリティ対策

1. 会社概要

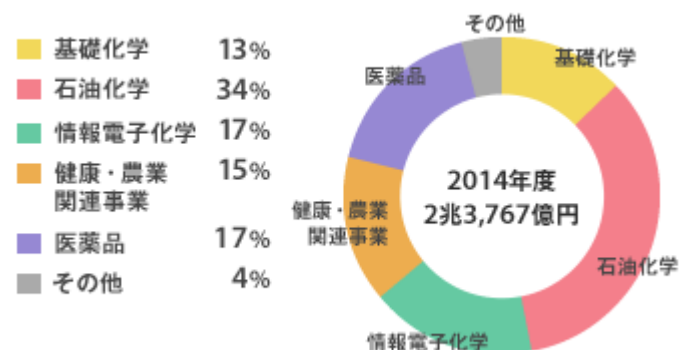
会社名	住友化学株式会社
創業	1913年 09月22日
営業開始	1915年10月 04日
設立	1925年 06月 01日
資本金	89,699百万円 (2015年03月31日現在)
本社所在地	● 東京 〒104-8260 東京都中央区新川2丁目27番1号 東京住友ツインビル東館 ● 大阪 〒541-8550 大阪市中央区北浜4丁目5番33号 住友ビル

● 従業員数(連結) 31,039名 (2015年03月31日現在)

● 2014年度実績(連結)

売上高	23,767億円	設備投資額	842億円
経常利益	1,574億円	研究開発費	1,479億円
当期純利益	522億円		

● 2014年度 部門別売上構成(連結)



2. 制御システムセキュリティ対策の背景

- セキュリティリスクが拡大
 - IP通信の普及と汎用OSの利用拡大
 - USBを介した感染事例が発生（Conficker等）
 - 標的型攻撃を行うマルウェアの登場（Stuxnet等）
- 国のサイバーセキュリティに関する施策
 - 2014年7月 **化学**が重要インフラ事業者指定される
 - 2015年1月 サイバーセキュリティ基本法の全面施行
 - 2015年9月 サイバーセキュリティ戦略の閣議決定
 - 2015年12月 サイバーセキュリティ経営ガイドライン公表

3. 制御システムセキュリティ対策の経緯

- 2013年度 セキュリティ主管部門を一本化
- 2014年度 石化協情報通信委員会情報セキュリティワーキンググループに参画
（重要インフラ事業者として活動開始）
- 2014年度 制御システムセキュリティワーキンググループ設立
- 2014年度 制御システムセキュリティ安全性調査を実施
- 2014年度 外部記憶媒体等の取扱いガイドライン制定
- 2015年度 安全性調査結果に基づき具体的な対策を検討

4. 制御システムセキュリティの特徴

- (1)セキュリティ3要素（機密性、完全性、可用性）のうち、特に可用性要求が高い。
- (2)システムのライフサイクルが長く、新旧システムが現場に混在している。



特徴にマッチした、現実的なセキュリティ対策が必要（多層防御）

5. 問題意識・課題と対応

5.1 問題意識・課題

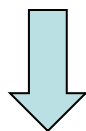
抱えている問題：

制御システムセキュリティ活動に対する体系だった取組みが出来ていない。

- (1)管理する組織が無い。
- (2)現状把握ができていない。
- (3)拠り所となるリファレンスモデルが無い。
- (4)管理すべき対象が明確になっていない。
- (5)技術・情報の伝承への不安を抱えている。

5.2 問題意識・課題への対応

(1)管理する組織が無い。

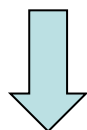


- ①制御システムを含んだセキュリティ主管部門を一本化。
- ②制御システムセキュリティWG設立。
- ③社内CSIRT(*)設立。

(*) : Computer Security Incident Response Team

5.2 問題意識・課題への対応

(2)現状把握ができていない。

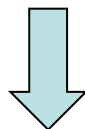


国内の全工場について、セキュリティ安全性調査を実施。

5.2 問題意識・課題への対応

(3) 拠り所となるリファレンスモデルが無い。

- ① 業界のセキュリティへの取組み状況把握ができていない。
- ② 制御システムセキュリティマネジメントシステムのリファレンスモデルを決めていない。
- ③ 工場毎にネットワーク構成がバラバラ



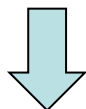
- ① 石油化学工業協会情報通信委員会情報セキュリティワーキンググループに参画
- ② 石油化学工業協会の安全基準をリファレンスモデルとして、
制御システムマネジメントシステム構築準備中
- ③ ISA 95機能階層モデル、および、ISA 99セキュリティモデルを
リファレンスモデルとしてネットワーク再構築準備中

5.2 問題意識・課題への対応

(4)管理すべき対象が明確になっていない。

(5)技術・情報の伝承への不安

- ・守っていくべき制御系の機器やソフトウェアの現状を表した一覧が無い
インシデント発生時に影響範囲特定等に手間取り、対策や更新を実施すべき対象機器やソフトウェアの一覧もすぐにリストアップされない。
DCSベンダからの完成図書には、機器やソフトウェアの一覧があるが、変更が重なってくると、つぎはぎだらけになり、現状のプラントの機器や、機器に搭載されたソフトウェアが何なのかが不明瞭になっている。
- ・技術、情報の伝承への不安
ベテラン計装エンジニア、システムエンジニアの引退やグローバル対応等に伴う人材の流動化
→プラント計装やシステムの維持管理業務を、これまでと同じやり方で継続することが
厳しくなりつつあり、属人的な仕事からの脱却が急務



対応：プラントの現状を表すものとして、制御システムの資産棚卸しを実施し、
機器やソフトウェアの管理台帳とネットワーク構成図を1対1で対応付けて
整備、見える化し、組織的な業務遂行を可能にする。

5.3 問題意識・課題への対応まとめ

抱えている問題： 制御システムセキュリティ活動に対する体系だった取り組みが出来ていない。

(1)管理する組織が無い。

- ①2013年度 制御システムを含んだセキュリティ主管部門を一本化
- ②2014年度 制御システムセキュリティワーキンググループ設立
- ③2015年度 社内CSIRT設立

(2)現状把握ができていない。

- ①2014年度 国内の全工場を対象にセキュリティ安全性調査を実施
- ②2015年度 セキュリティ対策後の期待効果を算出

(3)拠り所となるリファレンスモデルが無い。

- ①2014年度 石油化学工業協会情報通信委員会情報セキュリティワーキンググループに参画
- ②2015年度 石油化学工業協会の安全基準をリファレンスモデルとして、
制御システムマネジメントシステム構築準備中
- ③2015年度 ISA 95機能階層モデル、および、ISA 99セキュリティモデルをリファレンスモデルとして
ネットワーク再構築準備中

(4)管理すべき対象が明確になっていない。

(5)技術・情報の伝承への不安を抱えている。

- ①2015年度 プラントの現状を表すものとして、制御システムの資産棚卸しを実施し、
機器やソフトウェアの管理台帳とネットワーク構成図を1対1で対応付けて
整備、見える化し、組織的な業務遂行を可能にする。

6. 制御システムセキュリティ対策

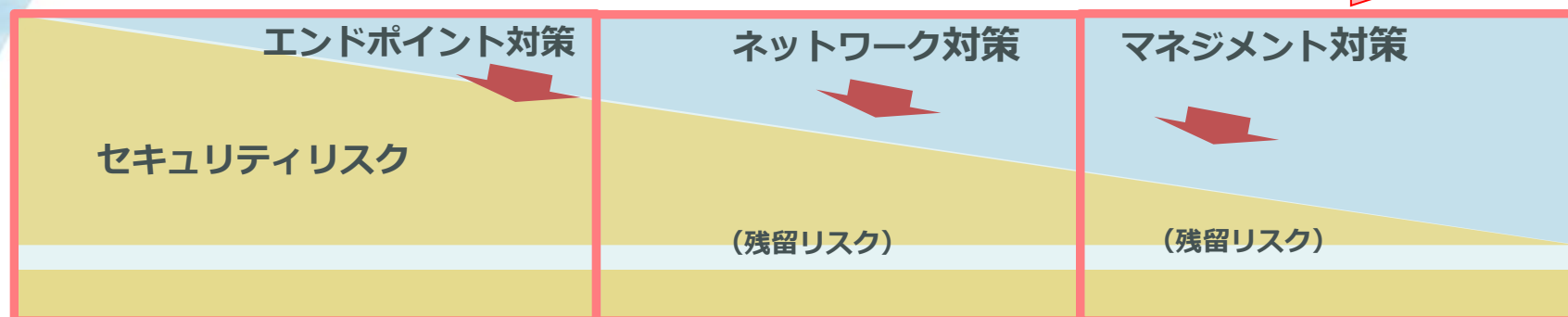
豊かな明日を支える 創造的ハイブリッド・ケミストリー



制御システムのセキュリティ安全性調査



対策の検討順序



制御システムの資産情報棚卸調査

エンドポイント対策

機器単体で実施する対策

- ・ パソコン、サーバ
- ・ ネットワーク制御機器

ネットワーク対策

ネットワークで実施する対策

- ・ ISA-99セキュリティモデル準拠の構造
- ・ IDS/IPSの強化
- ・ ログ解析
- ・ 冗長化

マネジメント対策

制度運用・教育等を通じて実施する対策

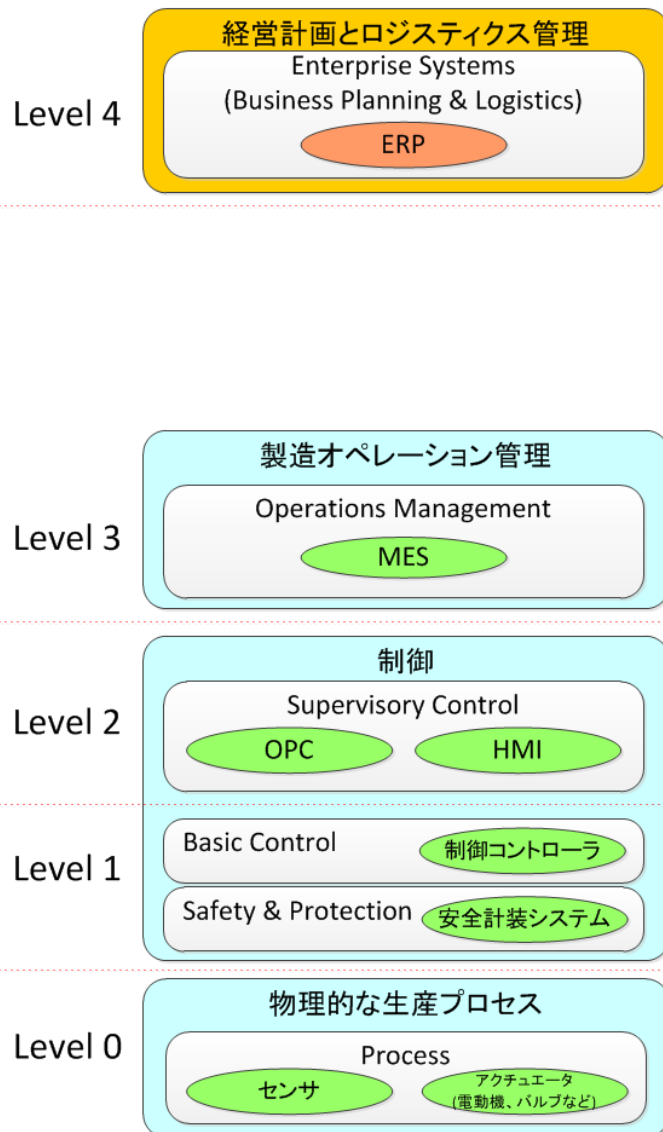
- ・ OA/FA/LAのポリシー本化
- ・ 石化協セキュリティ安全基準に準拠
- ・ 対策の内容を技術基準と運用基準に整理
- ・ 全社ルールと工場ルールの整合

ISA 99 セキュリティモデル

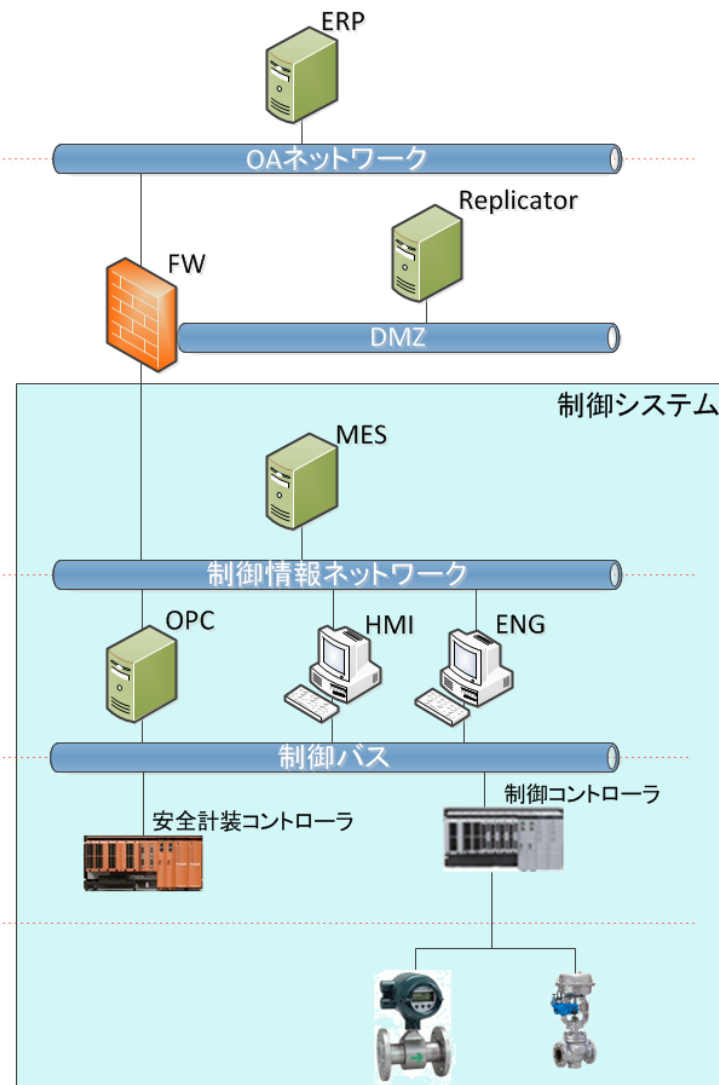
豊かな明日を支える 創造的ハイブリッド・ケミストリー



ISA 95 機能階層モデル



ISA 99 セキュリティモデル



※IACS = Industrial Automation & Control Systems