

通商産業省委託事業

大規模プラント・ネットワーク・セキュリティについて

～重要システムのサイバーテロリズム・クラッキング対策のあり方～

最終報告書

平成12年3月

大規模プラント・ネットワーク・セキュリティ対策委員会

まえがき

情報化社会の到来により、情報通信ネットワークが身近なものとなり、個人のパソコンから通信ネットワークを通して欲しい情報が誰でも何時でも容易に入手できるようになりました。このような環境のもとで、企業活動に関係する方々は、日頃扱っている企業情報を関係者以外には秘密にしておくように、情報を的確に管理することが重要になって来ています。企業組織として、情報通信ネットワークを介して企業活動を行う環境を整備し、企業の効率を向上することがグローバルな企業間競争の中で生き残っていくために不可欠なものになっています。このためにオープンな環境で企業の効率を上げる努力をするとともに、その弊害として通信ネットワークが各種の不正アクセスに晒される危険が増大しており、これらに対して如何に防御するかは、緊急かつ重要な課題となっています。

このことに関して、製造業を含む多くの企業がすでに、管理、技術の両面において然るべき対応がなされています。電力、ガス、石油、その他の大規模プラントでも、情報通信ネットワークとの関係を持ちながらオペレーションを行っており、オープン化の進む中、特にライフラインに関係している大規模プラントにおいては、つねに不正アクセスから防御し、プラントの安定操業を保持していくことが求められています。幸いなことに現在までサイバーテロからアタックされた事例は報告されていませんが、絶えず予防的措置を施しておくことが必要であります。

本委員会は、一般的な情報通信ネットワークに関するセキュリティ対策はすでに多くの検討と然るべき対応がなされていることを踏まえて、これらに包含されていないプラントの運転、制御、管理を対象にして、調査、研究を行うことにしました。本委員会は、平成9年度から上記の状況を認識し、問題の所在、取るべき対応策などについて調査、研究を行い、平成10年3月には、事柄の緊急性と重要性を考慮して、開発を必要とする技術的対応なども含めた中間報告書をまとめ、公開しました。その後も調査、研究を継続し、平成11年度末を目処に本委員会活動を終了することとして、中間報告書に織り込まれた内容を一部サマリーとして取り込みながら、最終的な成果物として本報告書をまとめました。本報告書をもって、この分野の仕事が終了し大規模プラントのネットワークセキュリティ対策が万全なものになったと言うことではないので、今後も絶えず新たな対応に迫られることが予想されます。残された課題もある程度明らかになっておりますので、別途、関連する活動は継続していく必要があると思われれます。

このようなことについて多くの方々に関心をもっていただくとともに、す

でに関心を持って関連の仕事を遂行されている方々に種々の面で本報告書が参考になれば関係者にとって幸いであると思います。

大規模プラントネットワークセキュリティ対策委員会
委員長 梅田 富雄

< 目次 >

まえがき

目次

委員名簿

委員会開催日程

第1章	中間報告書のサマリー	1
1.1	本委員会の背景と問題意識（本委員会設立の経緯）	1
1.2	本委員会の進め方	4
1.3	早急に講ずべきサイバーテロリズム・クラッキング対策	6
1.4	セキュリティレベル向上のための提言	9
第2章	中間報告後の活動の概要	11
2.1	検討課題と活動の進め方	11
2.2	活動の概要	12
(1)	防止技術の研究開発の企画	12
(2)	リスク分析手法の研究開発の企画	12
(3)	セキュリティ運用ガイドラインの策定	13
(4)	セキュリティ評価基準の策定	14
(5)	セキュリティ・マネージメントの研究	14
(6)	国際会議	16
第3章	非技術的事項の報告	17
3.1	セキュリティ・マネージメント	17
3.1.1	情報セキュリティ・マネージメント	18
(1)	情報セキュリティ・マネージメントの位置付け	18
(2)	リスク管理とリスク回避	19
(3)	セキュリティとセーフティ	22
(4)	情報セキュリティ理論研究と方法論の確立	23
(5)	情報セキュリティ・マネージメント標準化	24
(6)	セキュリティ・ポリシーの概念	24
(7)	情報閲覧とセキュリティ	27
3.1.2	サイバーテロリズムの理解	29
(1)	サイバーテロリズムの定義	29
(2)	脅威分析	31

3.1.3	国際協力の必要性	33
3.1.4	その他	34
(1)	専門家の早期育成	34
(2)	コミュニケーションギャップ	34
3.2	セキュリティ運用ガイドライン	36
3.2.1	運用ガイドラインの策定	36
(1)	運用ガイドラインの策定の意義	36
(2)	運用ガイドラインの策定の方法	36
(3)	不正アクセス対策基準の改訂	36
(4)	侵入経路別セキュリティ対策の運用ガイドラインへの適用	39
(5)	セキュリティ対策を実施する者の定義の見直し	40
(6)	用語の追加等	40
3.2.2	今後の課題	41
第4章	技術的事項の報告	45
4.1	セキュリティ技術開発	45
4.1.1	中間報告書で提案された対策の再検討	45
(1)	技術的再検討と掘り下げ	45
(2)	研究開発すべき技術について	45
4.1.2	開発テーマの選定作業	46
(1)	選定手順	46
(2)	選定結果	47
4.1.3	選定作業中に判明した事	49
(1)	現在利用可能とした技術について	49
(2)	研究開発すべきとした技術について	49
4.1.4	テーマ選定結果	50
4.1.5	まとめ	51
4.2	セキュリティリスク分析手法	53
4.2.1	問題意識	53
(1)	対象システム範囲の決定	54
(2)	対象リスクの決定	55
(3)	実施時期の決定	56
4.2.2	検討内容	56
4.2.3	検討結果	57
(1)	HAZOP の適用	57

(2) FTA/ETA の適用.....	59
4 . 2 . 4 提言、残された課題.....	66
4 . 3 セキュリティ評価基準.....	68
4 . 3 . 1 背景.....	68
4 . 3 . 2 コモン・クライテリア概説と活動概要.....	69
(1) コモン・クライテリア概説.....	69
(2) 活動概要.....	73
4 . 3 . 3 想定するモデル (TOE)	75
4 . 3 . 4 脅威と対策機能の洗い出し.....	78
4 . 3 . 5 プロテクション・プロファイル (PP)	82
4 . 3 . 6 成果.....	82
4 . 3 . 7 課題.....	82
(1) システムを対象とする PP を記述することに内在する課題.....	82
(2) PP 記述形式上の課題.....	83
(3) 個別機器の PP 検討への発展可能性.....	83
第 5 章 今後の課題.....	84
あとがき.....	86

[資料編]

- 資料 1 中間報告書 (平成 1 0 年 3 月)
- 資料 2 WG 活動報告 (中間報告後)
- 資料 3 国際会議発表資料 (平成 1 1 年 1 0 月 1 日)
- 資料 4 用語解説・和英対訳

委員名

本委員会委員

97 98 99

委員長	梅田 富雄	千葉工業大学・プロジェクトマネジメント学科・主任教授（プロセスシステム工学） 石油学会経営情報部会会長
委員	朝倉 義昭	東洋エンジニアリング株式会社・原子力電力事業部・副事業部長
	阿部 信夫	出光興産株式会社・製造部システム技術センター・主任部員
	磯村 順二郎	株式会社磯村国際関係事務所・代表取締役
	江木 紀彦	ITエンジニアリング株式会社・代表取締役社長
	高木 洋	王子製紙株式会社・技術本部技術部・技師
	河田 克哉	王子製紙株式会社・技術本部技術部・技師
	川村 理	三菱化学株式会社・技術部・部長
	川村 継夫	三井化学株式会社・システム部・部長補佐
	松岡 豊	三井化学株式会社・生産技術部・部長
	新井 弘志	山武ハネウエル株式会社・工業システム事業部・開発本部・課長
	木内 誠	山武産業システム株式会社・マーケティング部・グループマネージャ
	越島 一郎	千葉工業大学・プロジェクトマネジメント学科・助教授
	酒井 博満	東京電力株式会社・火力部設備技術グループ制御技術担当課長
	長井 昭二	東京電力株式会社・火力部設備技術グループ制御技術担当課長
	川島 哲哉	横河電機株式会社・制御システムセンター・開発2部
	加納 俊之	横河電機株式会社・制御システムセンター・開発2部長
	田中 俊明	横河電機株式会社・インダストリアルオートメーション事業本部・システム事業部・システム開発センター2部・部長
	壺井 彰久	株式会社NTTデータ・技術開発本部
	柳沢 光保	株式会社CRC総合研究所・公共システム事業部・主席研究員
	中澤 甫夫	株式会社CRC総合研究所・ネットワーク事業部・部長役
	西川 浩	住友化学システムサービス株式会社・技術開発本部・技師長
	花島 勝美	株式会社日立製作所・大みか工場・産業システム設計部・主任技師
	檜 豊太郎	日石三菱精製株式会社・根岸製油所・システムグループマネージャ

福山 真一	横河電機株式会社・システム事業部・マーケティング部・課長
松尾 正浩	コンピュータ緊急対応センター・運営委員
丸山 壽一	株式会社東芝・電機事業本部・プラント計装システム技術部・主査
村田 光一	東燃株式会社・システム部・部長
本橋 和夫	株式会社富士通システムソリューションズ・千葉第二システム事業部長
山口 義一	三菱電機株式会社・情報技術総合研究所・リアルタイムシステム部・チームリーダー
山崎 博	日揮株式会社・プロジェクトシステム本部・システム技術部・担当部長
横山 滋	日石三菱株式会社・情報システム部・マネージャー
新杉 寿康	日石三菱株式会社・技術部・製油技術グループ・担当課長
米司 実	日本製紙株式会社・技術本部・設備技術部・主席技術調査役
三浦 雅	日本製紙株式会社・技術本部・設備技術部・主席技術調査役
服部正志	新日本製鐵株式会社・技術開発本部・システム制御技術部長
米田 年	新日本製鐵株式会社・技術開発本部・システム制御技術部システム制御技術グループ・部長代理

オブザーバー

安延 申	通商産業省・機械情報産業局・情報処理振興課長
原山 保人	通商産業省・機械情報産業局・情報処理振興課長
小橋 雅明	通商産業省・機械情報産業局・情報セキュリティ政策室長
東井 芳隆	通商産業省・機械情報産業局・情報国際協力室長
鈴木 寛	通商産業省・機械情報産業局・情報処理振興課・課長補佐
江崎 禎英	通商産業省・機械情報産業局・情報処理振興課・課長補佐
向 賢一郎	通商産業省・機械情報産業局・情報処理振興課・課長補佐
桑原 敦	通商産業省・機械情報産業局・情報処理振興課・課長補佐
澤野 弘	通商産業省・機械情報産業局・情報処理振興課・安全指導係長
石井 伸治	通商産業省・機械情報産業局・情報処理振興課・安全指導係長
中村 達	情報処理振興事業協会・セキュリティセンター・不正アクセス対策室長
岸田 明	情報処理振興事業協会・セキュリティセンター・不正アクセス対策室長
宮川 寧夫	情報処理振興事業協会・セキュリティセンター・不正アクセス対策室・システム監査技術者
鈴木真理子	情報処理振興事業協会・セキュリティセンター・不正アクセス対策室

事務局	内山 政人	情報処理振興事業協会・セキュリティセンター・参事役
	長幅 朱美	情報処理振興事業協会・セキュリティセンター・不正アクセス対策室
	奥田 和男	日本情報システム・ユーザー協会・常務理事
	池谷 金吾	日本情報システム・ユーザー協会・企画担当部長
	角田 千晴	日本情報システム・ユーザー協会・調査広報担当・マネージャ

分科会メンバー（97年）

ユーザ企業分科会

リーダー	村田 光一	東燃株式会社
メンバー	檜 豊太郎	日本石油株式会社
	阿部 信夫	出光興産株式会社
	川村 理	三菱化学株式会社
	川村 継夫	三井化学株式会社
	酒井 博満	東京電力株式会社
	高木 洋	王子製紙株式会社
	西川 浩	住友化学システムサービス株式会社
	服部 正志	新日本製鐵株式会社
	横山 滋	日本石油株式会社
	米司 実	日本製紙株式会社
	磯村順二郎	株式会社磯村国際関係事務所
	岸田 明	情報処理振興事業協会

ベンダ企業分科会

リーダー	福山 真一	横河電機株式会社
メンバー	川島 哲哉	横河電機株式会社
	新井 弘志	山武ハネウエル株式会社
	加納 俊之	横河電機株式会社
	花島 勝美	株式会社日立製作所
	丸山 壽一	株式会社東芝
	本橋 和大	富士通株式会社
	山口 義一	三菱電機株式会社
	柳沢 光保	株式会社CRC総合研究所
	中村 達	情報処理振興事業協会

エンジニアリング企業分科会

リーダー	朝倉 義昭	東洋エンジニアリング株式会社
メンバー	壺井 彰久	NTTデータ通信株式会社
	江木 紀彦	千代田化工建設株式会社
	山崎 博	日揮株式会社
	松尾 正浩	コンピュータ緊急対応センター
	宮川 寧夫	情報処理振興事業協会

関連WGメンバー（98年、99年）

WG 1：セキュリティ技術開発

リーダー	岸田 明	情報処理振興事業協会
メンバー	新井 弘志	山武産業システム株式会社
	梅田 裕二	株式会社東芝
	小川永志樹	横河電機株式会社
	加賀 武志	新日本製鐵株式会社
	勝山光太郎	三菱電機株式会社
	金子 茂則	株式会社日立製作所
	川村 理	三菱化学株式会社
	才所 敏明	株式会社東芝
	花島 勝美	株式会社日立製作所
	福山 真一	横河電機株式会社
	藤井 稔久	山武産業システム株式会社
	米司 実	日本製紙株式会社
	米田 年	新日本製鐵株式会社

WG 2：リスク分析手法

リーダー	越島 一郎	千葉工業大学
メンバー	伊良部 猛	千代田化工建設株式会社
	鈴木真理子	情報処理振興事業協会
	西川 浩	住友化学システムサービス株式会社
	前嶋 玲子	千代田化工建設株式会社
	山崎 博	日揮株式会社
	アドバイザー	梅田 富雄

WG 3：運用ガイドライン

リーダー	檜 豊太郎	日石三菱精製株式会社
メンバー	朝倉 義昭	東洋エンジニアリング株式会社
	川村 継夫	三井化学株式会社
	木内 誠	山武産業システム株式会社
	酒井 博満	東京電力株式会社
	鈴木真理子	情報処理振興事業協会
	田中 俊明	横河電機株式会社
	花島 勝美	株式会社日立製作所
	羽生 浩明	株式会社日立製作所
	丸山 壽一	株式会社東芝
	横山 滋	日石三菱株式会社

WG 4 : 評価基準

リーダー	宮川 寧夫	情報処理振興事業協会
メンバー	阿部 信夫	出光興産株式会社
	内山 政人	情報処理振興事業協会
	奥原 雅之	富士通株式会社
	川村 理	三菱化学株式会社
	末延 忠明	富士通株式会社
	壺井 彰久	株式会社NTTデータ
	中澤 甫夫	株式会社CRC総合研究所
	配島 正道	株式会社CRC総合研究所
	松尾 正浩	コンピュータ緊急対応センター
	山口 義一	三菱電機株式会社

WG 5 : セキュリティ・マネージメント

リーダー	磯村順二郎	株式会社磯村国際関係事務所
メンバー	江木 紀彦	ITエンジニアリング株式会社
	木内 誠	山武産業システム株式会社
	岸田 明	情報処理振興事業協会
	越島 一郎	千葉工業大学
	中澤 甫夫	株式会社CRC総合研究所
	福山 真一	横河電機株式会社
	松尾 正浩	コンピュータ緊急対応センター
	丸山 寿一	株式会社東芝
	本橋 和大	株式会社富士通システムソリューション
	山崎 博	日揮株式会社
アドバイザー	梅田 富雄	千葉工業大学

委員会開催日程（平成9・10・11年度）

	開催期日	議 題
<平成9年度>		
第1回	平成9年 9月2日	報告： <ul style="list-style-type: none"> ・重要社会施設に対するサイバーテロリズムの脅威 ・プロセス制御系システムにおけるセキュリティ対策の在り方 ・セキュリティの観点から見た石油精製システムの現状 ・海外でのセキュリティへの要求事例
第2回	9月19日	報告：
第3回	9月30日	<ul style="list-style-type: none"> ・米国の電力系制御システムにおけるセキュリティ対策の現状 ・米国のサイバーテロリズム対策 ・我が国の石油会社におけるネットワークとセキュリティ対策の現状 ・我が国の製紙会社におけるネットワークとセキュリティ対策の現状 ・我が国の化学会社におけるネットワークとセキュリティ対策の現状 ・我が国の電力会社におけるネットワークとセキュリティ対策の現状 ・我が国の製鉄会社におけるネットワークとセキュリティ対策の現状 ・我が国の通信会社におけるネットワークとセキュリティ対策の現状 ・日本での最新の不正アクセスとウィルスの動向
第4回	10月17日	報告： <ul style="list-style-type: none"> ・我が国のプロセス制御系ベンダのセキュリティ対策の現状 ・我が国のプラントエンジニアリング企業のセキュリティ対策の現状 ・セキュリティ・マネジメントについて
第5回	11月5日	討議： <ul style="list-style-type: none"> ・ユーザ企業分科会の今後の指針について ・ベンダ企業分科会の今後の指針について ・エンジニアリング企業分科会の今後の指針について 報告：米国重要インフラ保護委員会の答申
第6回	11月20日	討議：
第7回	12月11日	<ul style="list-style-type: none"> ・ユーザによるセキュリティポリシーの設定と運用管理基準の検討 ・制御系システムで想定される脅威と侵入経路に関する分析 ・脅威の侵入経路毎に必要な技術・運用対策の検討 ・HAZOP手法を用いた通信系不具合の分析 ・今後の課題と提言
第8回	平成10年 1月27日	

<平成10年度>		
第1回	平成10年 6月5日	平成10年度の活動計画
第2回	7月10日	各WGの活動計画
第3回	8月17日	(1)各WGの活動報告 (2)補正予算への対応について (3)各WGの9月以降の活動計画について
第4回	9月25日	(1)応募案件の確認 (2)その他案件(9月以降のWG活動計画)の確認
第5回	11月19日	(1)WG活動報告 前回以降の活動内容 委員会報告に記述する項目と内容 3月までの活動項目と活動内容の構想 (2)今後の活動計画の確認
第6回	平成11年 1月28日	(1)「重要インフラ保護に関する大統領令にかかわるカンファレンス」参加報告 (2)「プラント・ネットワーク・セキュリティ運用ガイドライン(案)」報告 (3)各WG活動計画の確認
第7回	3月4日	(1)各WGの報告 (2)平成11年度の活動に対する委員からの意見聴取結果 (3)委員会報告書の構成と作成日程
第8回	4月2日	各WGの報告
<平成11年度>		
第1回	平成11年 5月13日	(1)WG4報告 (2)運営委員会(役割、報告書、国際会議)
第2回	6月17日	(1)WG5(アンケート調査)報告 (2)WG2報告(デモ) (3)国際会議検討状況報告
第3回	7月19日	(1)WG2報告 (2)運営委員会報告(報告書) (3)分科会による公開報告書の検討
第4回	9月10日	(1)「共有資料」についての分科会検討結果 (2)シンポジウム、専門家会議の内容・分担・資料等の確認 (3)「第2次中間報告書」の確認 (4)「最終報告書」の編集計画の確認
第5回	9月27日	(1)シンポジウム、専門家会議の確認 (2)安全性検証実験報告

		(3)「最終報告書」の編集計画の確認
番外	10月1日	シンポジウム： 「重要インフラのセキュリティ」
第6回	10月2日	<p>専門家会議：</p> <ul style="list-style-type: none"> ・ <i>Network Security Technology</i> Dr. Stephen D. Bryen ・ <i>Development Plan for Plant Network Security Technology</i> Mr. Fukuyama ・ <i>Measuring Network Risk</i> Dr. Stephen D. Bryen ・ <i>New Risk Analysis Methodology Development for Network</i> Mr. Koshijima ・ <i>Non-technical Approaches to CIP</i> Dr. Irwin M. Pikus ・ <i>Establishment of Security guideline on plant network</i> Mr. Hinoki ・ <i>Application of ISO/IEC 15408 into Plant Network</i> Mr. Miyakawa ・ <i>Security of Networked System Shell companies --and Beyond--</i> Mr. Pieter van Dijken ・ <i>Security management in the Fibers and Chemical industry</i> Mr. Robert T. George ・ <i>Survey Report</i> Mr. Isomura
第7回	10月22日	<p>(1) 国際会議について (2) 最終報告書作成について (3) 今後の委員会活動について</p>
第8回	平成12年1月14日	<p>(1) 最終報告書のチェック (2) 執筆者の説明 (3) 今後の予定</p>
第9回	3月8日	<p>(1) 報告書の最終チェック (2) 今後の予定</p>

第1章 中間報告書のサマリー

石油精製、石油化学、電力、鉄鋼、紙パルプ等の、社会的に重要なインフラストラクチャーであり、これらを構成する大規模プラントでは情報ネットワークのオープン化とともに、従来以上に高信頼性が求められる。本委員会は、平成9年9月より、大規模プラント・ネットワークに対して、悪意ある侵入者によるデータ等の改ざんや破壊によるプラントの爆発や停止などの障害発生の可能性とそれへの対応策について検討を行ってきた。

その間、平成10年3月に中間報告書を取りまとめ、大規模プラント・ネットワークに関するセキュリティにつき問題提起するとともに、対策の方向性を提示した。中間報告書は本報告書の資料編に含まれている。以下に中間報告書のサマリーを述べる。

1.1 本委員会設立の経緯

本委員会の背景は、中間報告書の6ページにおいて、以下の通り説明されている。

近年の情報化の進展に伴い、経済・社会の多くの分野が業務の効率性、生産性の向上などのため、コンピュータ・ネットワーク・システムに依存するようになってきている。その結果、コンピュータ・ネットワーク・システムの機能が停止したり不完全になると、経済活動はもとより、国民生活全般に深刻な影響を及ぼすことになる。

いわゆるサイバーテロリズムなどの脅威に対し十分なセキュリティ対策をとることが、これからの高度情報通信社会の構築に不可欠である。

プラントのコンピュータ・ネットワーク・システムを構成している情報系システムと制御系システムは、単体の独立したコンピュータから専用線や専用プロトコルを用いた閉域接続のネットワークへ、さらには標準プロトコルを用いた開放型システム間相互接続へと発展してきている。

情報系システムのネットワーク・セキュリティ対策に関しては「コンピュータ不正アクセス対策基準解説書」(1996.11.15)等がすでに存在するので、本委員会では制御系システムを主対象として、クラッキングを主としたネットワーク・セキュリティ対策を検討した。

本委員会において取り扱っている「クラッキング」、「サイバーテロリズム」の内容は下記に示されており、それらが行われる状況には様々な目的が

あるとされている。

「クラッキング」とは

正規の認証を経ずにコンピュータ・ネットワーク・システムに悪意をもってアクセスを試みること。

「サイバーテロリズム」とは

ネットワークを通じて政府や産業に対して行われる敵対的な行動であり、大規模で組織的な不正アクセスを試みること。

米国等の専門家によって「グローバルな情報戦争」と定義されている。一定の政治・経済目的により、行政、金融、航空管制、電力等の公共のコンピュータ・ネットワーク・システムに不正侵入し、システム自体の誤動作、停止、破壊および重要情報の不正取得、改ざん、ウィルス投与等を引き起こすこと。

コンピュータ・セキュリティに関する意図的脅威の目的

- * 国家転覆や社会攪乱目的
- * 脅迫、恐喝等の営利目的
- * 産業スパイ等のビジネス目的
- * 怨恨による復讐目的
- * 趣味（達成感、優越感）目的

本委員会は、大規模プラントという重要なインフラのプラント制御系システムをいかに防御するか、という点に重点を置いている。この問題意識の前提には、大規模プラント・ネットワークシステムに含まれる制御系システムの変遷及び今後の傾向に関して重要視する必要性を認識していることが挙げられる。ここに当該部分（中間報告書10ページ以下）を再掲する。

制御系システムの変遷

第1世代	1970年代～ 1980年代後半	・ コンソール、コントローラともベンダ各社のOSを使用している。 ・ 制御系システムと情報系システムとの通信は、回線容量が小さく、1対1で接続されており、データ交換などのアプリケーション層の通信プロトコルはベンダ固有または接続の都度相互に決めて行われていた。
第2世代	1980年代後半 ～ 1990年代前半	・ コンソールのOSは主にUNIX、コントローラはベンダ独自のOSを使用している。 ・ Ethernet 接続は情報系LANや制御系情報LANの中

		<p>でもごく一部に限られており、パソコンのネットワークはまだ普及しておらず、社外へのインターネットなどのオープンな接続もほとんどない。制御LANはベンダ固有の通信プロトコルを採用している。</p> <ul style="list-style-type: none"> ・UNIX系OSとTCP/IPプロトコルに精通した者であればコンソールまでの不正侵入は可能である。但しコントローラへのクラッキングは対象プラントの制御系システムの構造を十分に知らないとは不可能である。
第3世代	1990年代後半(最近)	<ul style="list-style-type: none"> ・コンソールのOSはUNIX系およびWindows NT等の汎用OSを使用している。コントローラはベンダ独自のOSを使用している。 ・汎用OSのネットワーク技術を活用することにより、オープン化が進んでいる。 ・汎用OSのネットワーク技術に精通した者であれば、コンソールまでは比較的容易に侵入でき、パソコンを含む社内、社外のネットワーク接続の普及により、クラッキングの脅威が高まりつつある。

制御系システムの今後の傾向

全社レベルの情報系システムとの接続	ERP(Enterprise Resource Planning)パッケージの適用、情報系既存システムとの情報共有、等
プラントの情報系システムとの接続、高度化、分散化、統合化	PIMS (Plant Information Management System)の適用
オープン化	汎用技術の採用(フィールドバス、TCP/IP)
汎用化	専用OSから汎用OSへのシフト

大規模プラントネットワークの制御系システムは、現在もこのような方向に進展しており、これらは大規模プラント運用の効率化に伴う必然の流れであるといえよう。次章以下において詳しく提示される本委員会の検討は、これらの動向に伴うセキュリティ確保の問題に対処するためのものである。

1.2 本委員会の進め方

本委員会では、制御系システムの計画・開発・設計・構築や運用の立場でのそれぞれの経験を踏まえ、関連知識の共有化と活発な意見交換を行う目的で、後に示すようなモデルシステムを構成し、ユーザ企業、エンジニアリング企業、ベンダ企業の3つの「分科会」に分かれ検討を進めてきた。

以下は中間報告書13ページ以下に記されている各分科会の検討内容である。

(1) ユーザ企業分科会

本分科会は、全委員が共通基盤のもとで議論を進めるために、国内各ユーザ企業の現状のシステム構成に即したモデル・システム構成を設定し、また詳細部分を含め委員相互の理解を深めるため、用語の統一を図った。その上で、内外部からの脅威に対して「防御すべき項目」のリストアップ（セキュリティ・ポリシーの明確化）を行なった。またユーザの立場から今後必要となる運用管理の要件、ベンダやエンジニアリング企業への要求事項についても検討した。

(2) エンジニアリング企業分科会

本分科会は、制御系システムにおけるネットワーク・セキュリティのリスク分析を、プラント設計のエンジニアリングプロセスの一環として位置づけた。「プロセス・セキュリティ・エンジニアリング」としての作業フローの整理と、HAZOP、FTA、JRAMなどのプラント・リスク分析方法のネットワーク・セキュリティ・リスク分析への応用を試みた。

(3) ベンダ企業分科会

本分科会は、外部からの侵入方法とセキュリティ侵害事象との関連について分析した。その際、侵入経路別の脅威分析をFTAにより行い、現在利用可能な技術、方法によって侵入経路別に早急に講ずべきセキュリティ対策を提案した。また今後必要となる新規セキュリティ技術の開発に関する提言を行った。

1.3 早急に講ずべきサイバーテロリズム・クラッキング対策

国内各社の現状のセキュリティ対策では、今後情報ネットワーク・システムがよりオープン化した場合に、サイバーテロリストによる悪意ある侵入に対抗するには不十分であるとの認識が示された。

本委員会では、セキュリティ・ポリシーの設定、脅威分析を経て、侵入経路別にセキュリティ対策を検討し、各企業が現在利用可能な技術を使用して講ずべき必要最小限の対策をとりまとめた（中間報告書第3章27ページ以下）。その検討結果を要約すると以下の通りである。

1. セキュリティ・ポリシーの設定

セキュリティ・ポリシー設定の一例としてプラントの中で防御すべき項目の重要度を3段階に区分した。

重要度が最も高い項目としては、

- ・バルブを操作されない
- ・チューニングパラメータを改ざんされない
- ・制御用設定値や上下限值を変更されない
- ・制御LANを乱されない
- ・データファイルや制御プログラムを変更・破壊・不正取得されない

重要度（中程度）として、

- ・制御系情報LANを乱されない
- ・プロセスコンピュータの画面をフリーズされない
- ・データファイル（品質、レシピ等）が不正取得されない
- ・プロセスデータを不正取得されない

重要度（小程度）として、

- ・プロコンに侵入されない
- ・プロコンの運転データを不正取得されない

2. HAZOP、FTAによる脅威分析

- ・プロセス・セキュリティ・エンジニアリングのフレームワークが提案された。
- ・HAZOP、FTAによるセキュリティ評価のチェックリストが提案された。
- ・セキュリティ侵害事象と侵入方法との関連が整理され、FT分析図が示された。

3. 侵入経路別の脅威分析

プラント・ネットワークのシステム構成モデルにおける侵入経路と侵入後の脅威を分析した。脅威は次のように分類され、分析された。

- (1) ネットワークからの不正侵入
 - (a) 情報系 LAN
 - (b) ダイヤルアップ接続
 - (c) 無線応用ネットワーク
- (2) プラントの計画・設計・建設時における不正侵入
- (3) 保守・リモートメンテナンスにおける不正侵入
- (4) その他
 - (a) コンピュータ・ウィルスの侵入
 - (b) ソーシャル・エンジニアリングによる侵入

4 . 侵入経路別のセキュリティ対策

モデル・システムに基づく侵入経路別の脅威分析の結果、制御系システムにおいても、一般的な情報システム技術が多用されていることもあり、今後オープン化により大規模プラント・ネットワークへ侵入される可能性はかなり高くなることが判明した。

ユーザ企業、エンジニアリング企業、ベンダ企業が現在利用可能な技術を用いて実施すべき必要最小限のセキュリティ対策をまとめた。その主要なものを以下に示す。

- (1) 情報系システムとの接続における対策
 - ・セキュリティポリシーを設定し、厳守する環境を作る
 - ・制御系システムと情報系 LAN との間にファイヤウォールを設置する
 - ・制御系情報 LAN の運用管理を強化する
- (2) セキュリティポリシーを設定
 - ・情報系においてもネットワークのセキュリティポリシーを作り、運用している企業は少ない
 - ・プラントにおいては、安全に関するマニュアル、教育はなされている
 - ・啓蒙・教育からスタートしなければならない
- (3) ファイヤウォールの設置
 - ・情報系のコンピュータは数が多い、万が一侵入されることを考慮する
 - ・制御系システムと情報系システムとをファイヤウォールで分離する

(4) 制御系情報 LAN の運用管理

- ・ 下記の運用ガイドラインを制御系に適用する
 - 「情報システム安全対策基準」
 - 「不正アクセス対策基準」
 - 「コンピュータウイルス対策基準」
 - 「システム監査基準」
- ・ 機器の限定、情報系とのデータの限定など制御系特有の運用を行う

1.4 セキュリティレベル向上のための提言

現状の技術や運用レベルでは近い将来増大するであろうサイバーテロリズムやクラッキングの脅威に対抗するには不十分であるとして、今後のセキュリティレベルを向上させるため必要な対策について提言している。

1. プラント用セキュリティ・ガイドラインの策定
 - ・プラント用のセキュリティ運用ガイドラインの策定
(「不正アクセス対策基準」などの改訂)
 - ・プラント用のセキュリティ評価基準の制定
2. ネットワーク・セキュリティにおける脅威分析手法の実証
 - ・ネットワーク・セキュリティのリスク分析の実施
 - ・HAZOP、FTA、JRAMなどを基礎とした系統的な新たな手法の確立
3. 防止技術の研究開発
 - ・制御系システムへの認証技術の適用
 - ・高速暗号化技術の開発と実証
 - ・セキュリティ対策を施したDCSの開発検討
 - ・疑似アタックの実験
4. ネットワーク・セキュリティに関する普及啓発
5. まとめ

国民生活に重大な影響を及ぼす大規模な施設の、特にその制御系システムの構築や運用にあたっては、ネットワーク・セキュリティに十分な配慮を払う必要がある。

具体的には次の3点に留意しつつ、個別プラントの状況をチェックすることを推奨する。

ネットワーク及びシステムのセキュリティはユーザ、ベンダ、エンジニアリング企業三者の共同責任で構築し、そのための投資が必要であることへの認識が必要である。

ネットワークのオープン化は時流であり、オープン化を阻害する方向での解決を求めることなく、セキュリティを維持しながらオープン化を進めることが重要である。

閉ざされた専用システムといえども、昨今のネットワークは社内あるいは他部門となんらかの形態で接続されており、運用にあたっては関係者全員のセキュ

リティ意識の向上が必要である。

第2章 中間報告後の活動の概要

本委員会は、平成10年3月に中間報告書を取りまとめて以降、中間報告の提言に沿って検討してきた。その検討結果は次章以降で報告されるが、本委員会の活動の概要は次のとおりである。

2.1 検討課題と活動の進め方

中間報告書に示された提言に沿って、次の4つの検討課題を取り上げることとした。

- (1) 防止技術の研究開発の企画
- (2) リスク分析手法の研究開発の企画
- (3) セキュリティ運用ガイドラインの策定
- (4) セキュリティ評価基準の策定

上記4点の他、「セキュリティ・マネージメントの研究」を課題に追加し、また、本委員会の成果を発信する「国際会議」を課題の一つに加えた。

各課題毎に、「ワーキング・グループ」を構成してユーザー、エンジニアリング会社、ベンダーの横断的立場から検討を実施した。「ワーキング・グループ」の構成に際しては、本委員会委員の他に専門的な委員の参加を得た。

課題(1)および(2)については、本委員会の任務を研究開発の企画までにとどめ、研究開発そのものは、別組織で対応することとした。同様に、中間報告の提言にある「疑似アタックの実験」も別組織で対応することとした。

各WGの活動成果は、委員会の席上に報告され、委員全員によるレビューが行われた。委員会報告として、その結果が第3章、第4章に記述されている。また、詳細は資料編にWG活動報告として収録されている。

2.2 活動の概要

活動内容と成果は次章以降に詳述されるが、その概要は以下の通りである。

(1) 防止技術の研究開発の企画

対象とする防止技術の網羅性を検証するために下記に沿って実施した。

- ・ 中間報告書で取り上げられている対策を、技術的対策と非技術的対策に分類。
- ・ 技術的対策については、別途、技術の体系化を行い、それに従って分類。
- ・ 非技術的対策については、「運用」と「その他」に分類。
- ・ 中間報告書で取り上げられていない技術的対策の有無を確認し、必要があれば追加。

以上の検討作業により、既存の「現在利用可能な技術による製品」の変更、および新規開発機能テーマを選定し、機能仕様を示した。この機能仕様が、別組織による開発作業の基盤とされた。

また、上記新規開発機能仕様の提起のほか、中間報告書において「現在利用可能な技術」とした技術を制御系システムに採用するに当たっては、適用性、有効性、可用性の観点から再吟味が必要であることを提起した。これに基づいて、別組織による技術開発後のアタック実験が実施された。

(2) リスク分析手法の研究開発の企画

以下の2つをテーマとして活動した。

テーマ1：セキュリティ・エンジニアリングのフレームワーク

テーマ2：プラントネットワークに対するリスク分析手法

テーマ1については、プラント・ライフサイクルに則したリスク分析の位置付けとし、その課題の検討を行った。

プラント本体に対する保全処置は、プラント・セーフティ・エンジニアリングとして対応技術が確立されており、プラントライフサイクル（計画、設計、建設、運用フェーズ）にあわせた具体的な安全性分析がおこなわれている。プラントネットワークに対しても同様に、ライフサイクルに対応したリスク分析手法が求められる。リスク分析手法としては計画・設計フェーズのみならず、運用フェーズにおいても統一的に使用できる手法であることが望ましいとしている。

テーマ2については、定性的アプローチとツリーベース分析手法からHAZOPとFTA/ETAを選択し、プラント・ネットワークにおけるリスク分析への適用可能性について検討を行った。

HAZOPを応用した分析手法の検討では、概念設計フェーズまで実施し、FTA/ETAを応用した分析手法の検討では、プロトタイプの作成まで実施した。シミュレーションを通して以下の手法拡張が有効であることを示している。

- 1) プラント本体並びに情報ネットワークの統一的表現
 - ・トポロジーの統一構造化表現
 - ・脅威の統一構造化表現
- 2) 動的変化への対応
 - ・構造抽出の自動化
 - ・FT構造生成の自動化
- 3) 故障・障害波及への対応
 - ・イベント検出とイベント伝播経路探索の自動化

(3) セキュリティ運用ガイドラインの策定

現状では制御系システムのセキュリティレベルに対する認識が企業間で異なるため、求められるレベルに関する客観的な基準が必要であるとして、企業等の組織が実施すべき対策を取りまとめた。なお、実際の対応に当たっては各企業等が自らの実情に応じた自主基準を本基準に沿って策定することが望まれる。

策定の方法としては、前回の調査における既存対策基準への追加の提案を引き継いで、「コンピューター不正アクセス対策基準」(通産省告示)をプラント・ネットワーク用に改訂することとし、中間報告書に記されている侵入経路別対策と既存対策基準の項目との対応を整理し、新規に追加すべき事項を検討した。

その結果、追加項目のかなりの部分が現状の不正アクセス対策基準に既にある項目で代替できるため、実際に追加する項目は3項目のみであった。

また、大規模プラント・ネットワークの運用実態に則して、「セキュリティ対策を実施する者」(すなわち、「システムユーザ」、「システム管理者」、「リモートメンテナンス」)の定義を見直し、あわせて、プラント・ネットワークの運用に携わる者が理解し易いよう、対象となるネットワークを図示し、また、「情報系システム」、「制御系システム」、「大規模プラント・ネットワーク」など、対象となるプラント・ネットワーク固有の用語の定義を追加した。

(4) セキュリティ評価基準の策定

ワーキング・グループ4が活動を開始した時期、コモン・クライテリア (Common Criteria 以下CC) が国際的なセキュリティ評価基準の枠組みとして提案され、国際標準化されつつあった。

制御系システムのセキュリティの機能要件、すなわち当該システムに求められるセキュリティ機能を整理する枠組みをCCに求めた。CCの枠組みにおいて実際に評価基準に相当する部分はプロテクション・プロファイル (Protection Profile 以下PP) である。この枠組みは相当の客観性と普遍性が期待できると考えられたので、制御系システムに要求するセキュリティ機能要件をPPとして記述することができないかを検討した。

PPの策定には以下の作業が必要となる。

- 評価対象の規定
- 想定される脅威の抽出
- 対応する対策機能の列挙
- PP様式に則った整理

評価対象は、制御系システムというネットワーク・システムである。これについては抽象的な概念モデルを設定し、対象範囲を規定した。

想定される脅威については、中間報告において数々の「脅威」が認識されていたが、想定される「脅威」と対応する「対策機能」を対で洗い出すため、ブレン・ストーミングを繰り返して、両者を同時に整理した。

PP様式に則った整理については、実際に英語で記述することを試みた。困難な作業であったが、その結果、日本人の読者にとって読みやすい形態、項目の並びにはなっていないことが明らかになった。何らかの工夫が必要と思われる。

以上の成果としては、概念モデルとしての「制御系システム」を構成する主要な各機器がもつ「脅威」と「対策機能」の鳥瞰を得ることができた。

(5) 情報セキュリティ・マネージメントの研究

非技術系セキュリティ対策である情報セキュリティ・マネージメントは、費用対効果を考慮した現実的かつ有効的なセキュリティ対策を形成する観点から、技術系セキュリティ対策とともに車の両輪と考えられる。

情報セキュリティ・マネージメントの有効性は、情報系ネットワークのみならず制御系ネットワークにおいても同様である。しかしながら、制御系ネ

ネットワークにおいては情報セキュリティ・マネージメントが形成されていない。このテーマについて、海外調査を行い各国と意見交換を行うとともに、国際会議においても論議し、内外に向けた情報発信を行った。

この研究では、制御系ネットワークにおける情報セキュリティ・マネージメントにおける課題を洗い出した。

- ・サイバーテロリズムなどの脅威に対する認識
- ・セキュリティの経済価値に対する認識
- ・マネージメントのあり方の文化的背景
- ・法規制などの社会的背景

これに基づいて、以下の調査を実施した。

- ・情報セキュリティ・マネージメントの標準規格[英国標準規格 B S 7 7 9 9]の調査研究
- ・大規模プラント関連産業界の各企業における情報セキュリティ・マネージメントに関する意識、組織的対応体制、具体的対応内容等の実態調査
- ・海外の政府機関、セキュリティ機関、企業を対象に、制御系ネットワークの情報セキュリティ・マネージメントに関する訪問調査、意見交換

上記の調査の結果、情報セキュリティ・マネージメントに関して主な課題が下記のように挙げられた。

1 . 情報セキュリティ・マネージメント

- 情報セキュリティ・マネージメントの位置付け
- リスク管理とリスク回避
- セキュリティとセーフティ
- 情報セキュリティ理論研究と方法論の確立
- 情報セキュリティ・マネージメント標準化
- セキュリティ・ポリシーの概念
- 情報閲覧とセキュリティ

2 . サイバーテロリズムの理解

- サイバーテロリズムの定義
- 脅威分析

3 . 国際協力の必要性

4 . 課題

- 専門家の早期育成
- コミュニケーションギャップ

(6) 国際会議

平成 11 年 10 月 1 日の情報化月間行事の一翼を担って、シンポジウム「重要インフラのセキュリティ」を約 100 名の一般参加者を得て開催した。

シンポジウムにおける本委員会からの報告は、中間報告を中心に行われた。講師陣は、本委員会委員のほか国内および海外から招聘され、招聘講師は下記のとおりである。

国内招聘：江畑健介氏（軍事評論家）

海外招聘：

Dr. Irwin M. Pikus

Director, Communications and Information Infrastructure Assurance Program, U.S. Department of Commerce, NTIA

Dr. Stephen D. Bryen

Managing Partner, Aurora Marketing & Business Development

Mr. Robert T. George

Manager, Benchmarking Programs, DuPont Information Security Organization E.I. DuPont de Nemours & Co.

Mr. Pieter van Dijken

ITS (Information Security Services) Shell Services International B.V.

翌 10 月 2 日には、上記の海外招聘者を交えて、中間報告書発表以後のワーキンググループ活動成果の報告と、課題に関連した海外招聘者からの報告を議題とする専門会議を非公開で開催し、本委員会の活動に対する海外招聘者からの意見を聴取した。

具体的には、下記のテーマなどについてプレゼンテーションとディスカッションが行われた。

- * 技術系対策
- * リスク分析
- * 非技術系対策
- * ISO 15408
- * セキュリティ・マネジメント

第3章 非技術的事項の報告

3.1 セキュリティ・マネージメント

非技術系セキュリティである情報セキュリティ・マネージメントは、費用対効果を考慮した現実的かつ有効的なセキュリティを形成する観点から、技術系セキュリティとともに車の両輪である。加えて、情報セキュリティ・マネージメントは国際間での企業合併や提携、生産拠点の分散化などでよりグローバルなインフラとしてのネットワークが必要とされる環境下で、接続相互間の信頼性を備えた効率的な運用上欠かせないものである。

情報セキュリティ・マネージメントの有効性は、情報系ネットワークのみならず制御系ネットワークにおいても同様である。しかしながら、情報セキュリティ・マネージメントの形成確立に向けて数々の課題が残されていることは、99年2～3月に実施されたアンケート調査¹、99年2月に行われた海外調査²、99年10月の東京での国際会議³、および本委員会ワーキンググループ(WG)5の討議等でも明らかになっている。

本項では、制御系ネットワークにおけるサイバーテロリズム対策に焦点をあてた情報セキュリティ・マネージメントを検討したものであるが、当然ながら情報系ネットワークのセキュリティに対しても共通性のあるものである。

- 1 情報セキュリティ・マネージメント
 - (1) 情報セキュリティ・マネージメントの位置付け
 - (2) リスク管理とリスク回避
 - (3) セキュリティとセーフティ
 - (4) 情報セキュリティ理論研究と方法論の確立
 - (5) 情報セキュリティ・マネージメント標準化
 - (6) セキュリティ・ポリシーの概念
 - (7) 情報閲覧とセキュリティ
- 2 サイバーテロリズムの理解
 - (1) サイバーテロリズムの定義
 - (2) 脅威分析
- 3 国際協力の必要性

¹ 「重要社会インフラ産業におけるコンピュータおよびネットワークに関するセキュリティ・マネージメントアンケート調査」、資料編参照

² 海外調査報告書「海外の関係機関・企業の動向」、資料編参照

³ 資料編参照

4 課題

- (1) 専門家の早期育成
- (2) コミュニケーションギャップ

3.1.1 情報セキュリティ・マネージメント

(1) 情報セキュリティ・マネージメントの位置付け

情報セキュリティ・マネージメントは、ネットワークのパフォーマンスの低下を極力抑えてセキュリティを維持すると共に、情報の価値、品質、生産性の向上を図ることを目的とするものである。

コンピュータ・ネットワークは、「産業革命に匹敵する革命」とも言われ、産業のみならず、社会のあらゆる活動に大きな変革をもたらしている。今日の、そして将来のコンピュータ・ネットワークは確実に、『さまざまな文化や国家における脅威、仕事の進め方、プロセス、最新のプロセス制御コンピュータ、それにきわめて高度なグローバルネットワーク』⁴と結びついていく。そこを流通する情報はより一層、貨幣価値、権利価値、特許価値、商品価値などきわめて高い価値を有するものとなってくる。

情報セキュリティ・マネージメントは、特に欧州において発展してきた。『ヨーロッパでは、パブリック・オープン・スタンダードと呼べるものの制定を目的として政府と企業が協力してきた。ベンダーごと、技術ごとの取り組みではなく、パブリック・オープン・スタンダードによってこそ、セキュリティの問題に対処することができるという認識はきわめて明瞭である。技術的問題よりも、管理上の問題が大きい。これが BS7799 (情報セキュリティ・マネージメントに関する英国標準規格) の出発点であり、それをわれわれが信じている理由なのである』⁵

有効かつ効率的な情報セキュリティ・マネージメントは、組織内のすべての利用者が情報セキュリティ・マネージメントについての正しい理解と認識を持ち、決められたルールを正しく実行することが最も重要である。自動車に装備されているセーフティベルトやエアバッグが安全運転を保証するものではないのと同様に、情報セキュリティにおいても利用者がセキュアなオ

⁴ 国際会議のパネルディスカッションにおけるピエテル・ファン・デュヒケン氏の発言より

⁵ 同上

ペレーションを行うことが不可欠である。

情報セキュリティ・マネージメントは、情報系ネットワークは無論のこと制御系ネットワークにおいても実施されることが望ましい。組織全体で忠実に実施されることが肝要であり、トップ・マネージメントが明確な指示を設定した上で、支援と約束のもとに全社的取り組みがなされなければならない。

アンケート結果等から見ると、情報セキュリティ・マネージメントの意義、位置付けが十分に認知されていない。企業においては急速に発展するネットワークを有効な経営資源とし情報資産の価値を高めるために、トップ・マネージメントの指示のもと全社的な情報セキュリティ・マネージメントへの積極的な取り組みが望まれる。

情報セキュリティ・マネージメントは、単に外部の脅威から身を守るために「核シェルター」に身を潜め、装甲車でネットワーク上を行き交おうとするものではない。情報価値への認識を高め、より高い価値のある情報をネットワーク上で流通することによるビジネスの飛躍的発展と効率化を目指しており、そのための信頼性の高いマネージメントの確立を図るものである。情報価値の評価が行われることにより、ネットワーク上を流通する情報の品質も評価の対象となる。情報発信者は高品質、高価値の情報の発信を心がけなければならない。企業は、自社から発信される情報の品質管理を行うことが企業評価の重要な要素となってくる。また、情報価値の評価はあらゆるデバイスに死蔵している情報の掘り起こし、整理を促す。多量の死蔵情報はシステム資源の無駄遣いのみならず、セキュリティ管理上の死角となりやすい。ネットワークにおいても生産性の向上を図ることが重要であり、情報セキュリティ・マネージメントの重要な役割の一つである。

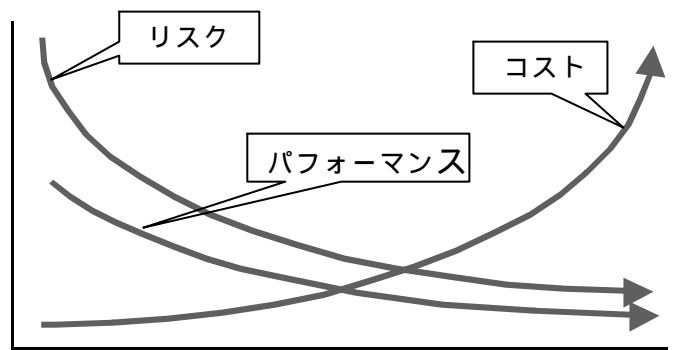
特に、セキュリティ対策をどの程度やればよいのか大きな不安を持ちながら手探りの対策をとらざるを得ない現状を鑑みると、情報セキュリティ・マネージメントは一つの解決を与えてくれるものと考えられており、その確立が急務でもあることを痛感する。

(2) リスク管理とリスク回避

セキュリティには、二つの基本的なアプローチがある。一つは「リスク回避」アプローチ、もう一つはいわゆる「リスク管理」アプローチである。

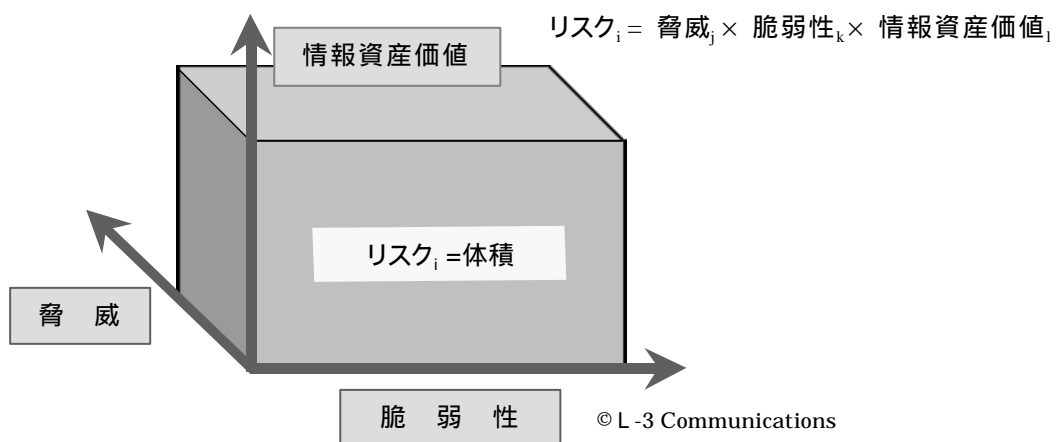
リスク回避アプローチは、セキュリティの専門家が用いる従来型のアプローチであり、国防関係では長年好まれてきた。リスク回避アプローチはトータルなセキュリティ・システムのことであり、現実の世界では非常に費用がかさみ、セキュリティに伴う手続きが多く、実際にはパフォーマンスが低下し業務の遂行が非常に難しくなる。しかも、実用面からみてセキュリティ・システムが常に機能するとは限らないという問題点もある。

リスク管理アプローチの理念は、コストの増加を抑制しつつパフォーマンスに悪影響を与えずにリスクを大幅に軽減できる中間領域をプロセスの中で見つけることである(図表 1)。情報セキュリティ・マネージメントで重要なことはリスクの管理である。リスクを査定する際の要素は、情報資産の価値、脅威、システムおよび組織の脆弱性であり、基本的にはその積がリスクとの考えられる(図表 2)。



© L-3 Communications

図表 1



© L-3 Communications

図表 2

リスク管理アプローチは、システム内の脆弱性を数えることでもなければ、ネットワークをスキャンし調査することでもない。また、単に不正侵入検知、ファイアウォールの設置、侵入テストの実施でもない。これらはすべて個々の保護手段に過ぎないものである。これらがコスト効率のよい手段となる場合も、まったく必要とされない場合もあり、いずれの場合においてもその有効性を十分に検討して決定を下す必要がある。

セキュリティ対策では、すべてのリスクを排除、あるいは回避しようとする考え方が主流を占めやすい。これは、リスク回避アプローチとは異なるものである。つまり、アプローチを検討するのではなく、空想的な願望であり、絶対的的要求である。特にわが国においてはユーザのみならず、世論、マスコミ、発注者、上司、トップ・マネージメントからのそのような願望や要求のもとで、セキュリティに関してのまともな議論が交わしにくい環境がある。このような環境下における議論では往々にして感情論が先行し、冷徹な脅威、リスク、脆弱性、情報資産価値の分析や対策の検討が排除される傾向がある。「すべてのリスクは排除され、回避されるべきである」という一見正論のようにも聞こえるこのような感情論と、まともに議論することは至難の業である。感情論は極論に走りやすく、「リスクを排除できないネットワークは危険である」という結論に導かれる危険がある。

コンピュータ・ネットワークはハードウェアやシステムのみならず、利用展開あるいは知識や情報の価値を含めて急速な発展途上にあり、それに対するセキュリティ対策も例外ではない。そのため、セキュリティを現在の技術レベルに基づいて固定目標として捕らえることははなはだ危険である。『今日適用されているセキュリティ手順、慣行、プロセスは、グローバルで、オープンシステムで、知識主導型となる明日のビジネス動向にとってはいずれ適切でなくなるだろう』⁶と考えられている。やみ雲な技術的歴史観の欠如したセキュリティ対策、あるいはリスク回避を法律と法執行機関に過度に依存することはネットワークのパフォーマンスを著しく低下させるのみならず、コンピュータ・ネットワークの発展そのものを阻害するものである。『情報化時代と言われる今日、われわれの業務における価値付加プロセスは知識と情報である。そのため、ふさわしくない人が当社の情報にアクセスすることよりももっといけないことは、ふさわしい人がアクセスできなくなることな

⁶ 国際会議のパネルディスカッションにおけるロバート・ジョージ氏の発言より

のだ。ふさわしい人がアクセスできるようにすることは非常に重要なことなのである』⁷。セキュリティ対策を検討する上での最大のリスクが、感情論や感情論の発信者であってはならない。

(3) セキュリティとセーフティ

わが国においては「セキュリティ」と「セーフティ」の概念的区別が明確ではない。双方共に「安全」と解されるが、セキュリティはわが国ではこれまで余り意識されてこなかったものである。特に、企業活動においては安全対策、保安対策としてのセーフティの概念はあるものの、セキュリティとの関わりは無かったに等しいためなおのこと捉えにくい概念である。

セキュリティとセーフティの定義の違いを明確にする事は非常に難しい課題である。明確に区別できる日本語もない。政治用語としては、セキュリティを「安全保障」としている。ドイツ語でも「Sicherheit」という一つの単語である。

一つの考え方としては、「セーフティは状態であり、それは危険から遠ざかり、危険から逃れる結果から得られるものである。セキュリティはセーフティを保障するために危険に対峙し、それを排除する、あるいは危険をコントロールするものである」といえる。

セキュリティはセーフティよりも広い概念を持つものであると考えられる。セキュリティが保障するものは、財産・資産の保障、生命の保障、信用保障、生産性の保障、権利の保障、人権の保障、名誉の保障、安全の保障などである。

セキュリティは「セキュアな状態、感覚。守ること、あるいは保障すること。国家や企業のスパイ、窃盗あるいは他の脅威（危険）に対する安全（セーフティ）。これを確実にするための組織」⁸と意味付けられているが、セキュリティとセーフティの概念の違いを実感として捉え、行動に結びつけるのははなはだ困難がともなう。

セキュリティは、セーフティに比べより能動的に脅威に対し防御する概念を持っているといえる。よって、ネットワークの能力を十分に発揮させ、業務に寄与するために、自己責任においてリスクの冷徹な分析評価を行い、セキュリティを維持することが重要である。特に、ネットワークはグローバル

⁷ 同上

⁸ The Oxford Encyclopedic English Dictionary

な規模で接続されているものであり、一つのセキュリティの欠陥がネットワークに繋がる多くのユーザに被害を及ぼすことに鑑み、それぞれが自己責任において一定水準以上のセキュリティを維持することが不可欠である。セキュリティは単に防犯を目的にするものではなく、ネットワークのパフォーマンスを維持し情報の品質と価値を高めるものであることを銘記しなくてはならない。

(4) 情報セキュリティ・マネジメント理論研究と方法論の確立

急速なネットワーク化による情報環境の変化に、マネジメントが追いついていないのが現状であろう。その中でも、情報セキュリティに対するマネジメントは最も遅れている領域である。そのため、情報セキュリティ理論研究と方法論の確立は今後のもっとも重要な課題である。

情報セキュリティは技術系セキュリティと非技術系セキュリティから成り立つことは前記している。つまり、セキュアなシステムを構築しネットワークのセキュリティを確保するための技術系セキュリティと、システムおよび情報のセキュアな運用を図るための非技術系セキュリティとしての情報セキュリティ・マネジメントである。

制御系ネットワークにおいても、情報系ネットワークと同様のセキュリティ・マネジメントが実施されなくてはならない。しかも、情報系、制御系ともに、企業における組織としての統一された情報セキュリティ・マネジメント基準の確立と実施が必要である。

情報セキュリティ・マネジメントの範囲はネットワーク上における情報のみならず、ネットワークの入出力情報、情報媒体の取り扱いを含めたものである。企業組織内のあらゆる情報管理を念頭に置いたものとなる。

国際的にもセキュリティ対策の現状には混乱と迷走が多々見受けられる。その背景には、情報セキュリティ理論研究が皆無に等しいことと、有効な方法論が確立されていないことがある。方法論がしっかりしていないために、セキュリティ対策が「泥縄式」になっていることは否めない。

技術系セキュリティにおいては、セキュリティ・ツールも数々開発されてきているが、セキュリティ方法論の中で重要なことはツール体系の確立である。ツールが体系化されることにより、ユーザは各々のツールの機能、役割、位置付けを明確に把握でき、有効な対策を推進できよう。

(5) 情報セキュリティ・マネジメント標準化

情報セキュリティ・マネジメントの標準化の動向としては、ISOで進められているGMITS(Guideline for the Management of IT Security)と英国標準のBS 7799(British Standard 7799)がある。

標準化はネットワークを通じた国際間の商取引が増大するのに伴い、企業間の相互接続性の信頼関係を確立するために必要となってくる。しかしながら、形式的な標準化は避けなければならない。あくまでも、標準化は有効な情報セキュリティを確立し、企業の信頼性を高め、生産性の向上を図るものでなくてはならない。

わが国としては、わが国の経営形態に則した標準化を確立することも重要な課題であるが、同時に国際的に互換性のあるものとすることも念頭におく必要がある。

また、GMITS、BS 7799共に情報系を対象にしたものであり、重要社会インフラのセキュリティにおいては制御系においても同様の国際的標準が必ずや必要となってくる。わが国は制御系ネットワークのセキュリティにおいては確実に他国より先行しており、制御系における情報セキュリティ・マネジメントの国際的標準の策定に向けてのイニシアチブをとらなければならない。

いずれにしても、国際的標準化作業は関係国の認識と思惑の違いがあり時間がかかるものと思われる。一方、BS 7799はシェル社をはじめ大企業や英国の金融機関で実際に使われており、そこで蓄積される経験は貴重である。

(6) 情報セキュリティ・ポリシーの概念

情報セキュリティ・ポリシーは、情報セキュリティ・マネジメントを行う上での基本方針を示し、情報セキュリティの目的、範囲、重要性を定義するものである。組織全体にトップ・マネジメントの情報セキュリティに対する考え方、姿勢を周知するための文書である。

アンケートの結果からは、実際に実効性のある情報セキュリティ・ポリシーが作成されている企業は1割以下に留まるものと見られる。

現在、情報セキュリティ・ポリシー作成にあたって二通りの考え方がある。

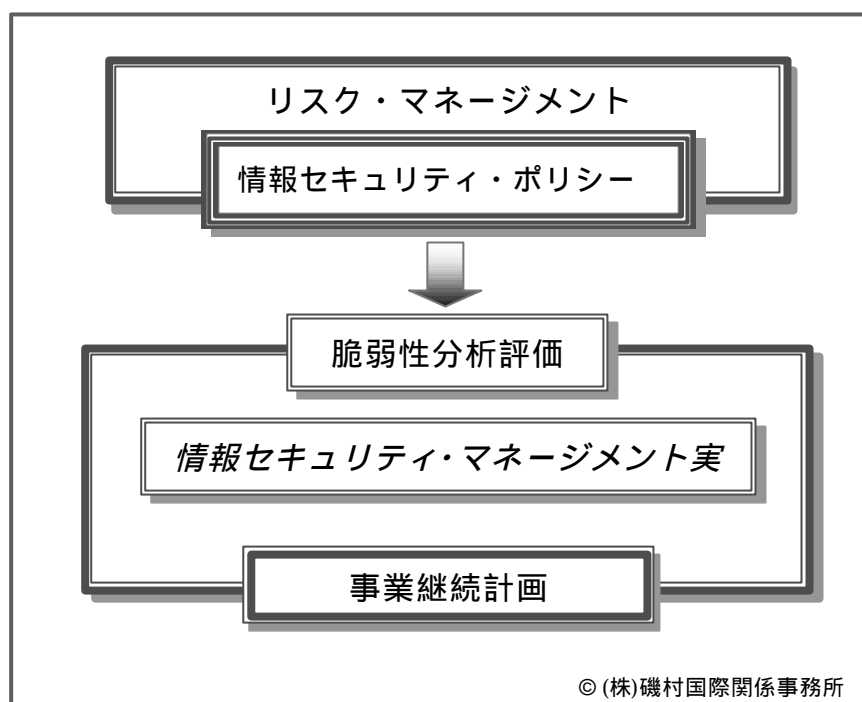
第一は米国の考え方に基づいたもので、情報セキュリティ・ポリシー＝情報セキュリティ・マニュアル（ガイドライン）であり、第二は英国のBS7799に基づいた、情報セキュリティ理念としての情報セキュリティ・ポリシーである。

第一のものは、マニュアルであるために相当の厚さになる。一方、第二のものは極端には1ページに集約され、多くても数ページである。

これは、米国と欧州における「ポリシー」の上位概念の差から生まれている。米国においては、「戦略」が上位概念であり、ポリシーは戦略を展開したものであり、欧州においては「ポリシー」が上位概念となる傾向がある。

企業内での情報セキュリティ・ポリシーの実務的な展開を考慮するならば、第二の情報セキュリティ・ポリシーの形態が望ましいと考えられる。情報セキュリティ・ポリシーはIT部門でのみ展開されるものではなく、トップ・マネジメントの意思と関与で作成され、組織全体で理解され実施されなくてはならないものである。マニュアル形式の情報セキュリティ・ポリシーの欠点はマニュアル提供側の論理に偏りすぎるきらいがあり、組織内のユーザ全体に有効に機能するとは考え難いからである。

情報セキュリティ・ポリシーは、トップ・マネジメントに司られるリスク・マネジメントのもとで作成されなければならない。作成にあたっては、ポリシー範囲の設定が求められる。情報セキュリティの広義な範囲としては、組織に帰属する書類、情報、電話、FAX、e-メール、郵便、廃棄書類（シュレッダーを含む）会話まで含まれる。コンピュータ・ネットワークの範囲においても、入出力情報、ネットワーク接続、アクセス、情報分類等の管理の範囲が確定されなければならない。



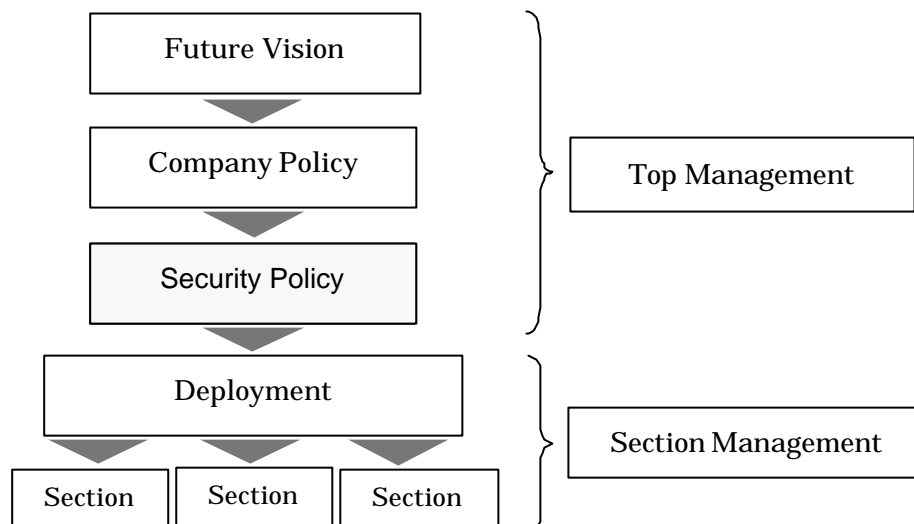
図表 3

決定された情報セキュリティ・ポリシーに基づいて、各セクションのマネージャは情報セキュリティ・マネージメントの具体的な展開を求められる。各セクションのマネージャは、先ずネットワークの脆弱性を分析把握し、それに基づいてマネージメントを行う。

情報セキュリティ・マネージメントで重要なことは、事業継続計画 (Continuity Plan あるいは Contingency Plan)の策定である。事業活動に対する障害に対処するための計画であり、重大な故障や災害等の影響から重要な事業プロセスを保護し、重大な障害が発生した場合の事業プロセスおよび業務の迅速な回復を行うためのものである。事業継続計画の基本構成要素は、緊急手順、フォールバック手順、回復手順、テストスケジュールである。(図表 3)

情報セキュリティ・ポリシーを入口とするならば、事業継続計画は出口に位置するものであり対を成す。アンケート結果からは、生産設備における安全保安対策上の事業継続計画は策定されているものの、コンピュータ・ネットワークのセキュリティを対象とした事業継続計画の策定はほとんどなされていないのが現状である。

10月に開催された国際会議での結論としては、情報セキュリティ・ポリシーの作成は企業の中長期ビジョン(Future Vision)をもった企業ポリシー(Company Policy)に基づいて作成されなくてはならない。また、情報セキュリティ・ポリシーの展開(deployment)は各セクションのマネージャが責任者として行わなくてはならないということである。(図表4)



図表 4

国際会議の招請講師であるピエテル・ファン・ディヒケン氏の発言は、シエル・インターナショナル社が1990年のBS7799パート1の開発段階から参加するとともに、実際のオペレーションに基づいた経験と実績からのものであり非常に重みのあるものであった。また、ロバート・ジョージ氏はデュポン社で同様の多くの実績を積み重ねてきており両社のセキュリティ・ポリシーの考え方は一致している。

(7) 情報閲覧とセキュリティ

国際会議において情報閲覧とセキュリティの関係においても討議が行われた。

TCP/IPというプロトコルは誰でもが情報を閲覧できるものであり、そのプロトコル上で情報へのアクセスを制限しようとするのは機能上相反することを目指すことになる。情報へのアクセス制限は、承認されたアクセス権を持つ者をも制限することにもなるので極力避けるべきである。

基本的には情報は積極的に開示すべきであり、重要な情報(プライバシー、

企業秘密等)へのアクセスのみを制限すべきである。

よって、将来の方向性としては情報開示を前提としたうえでの適切な情報のセキュリティ保護レベル分類を規定し、規定に従った情報の分類と各々の情報の管理者(情報のオーナー)が責任を有するもとの、重要情報へのアクセスに限り制限することが望まれる。

3.1.2 サイバーテロリズムの理解

(1) サイバーテロリズムの定義

サイバーテロリズムを論ずるには、まず、テロリズムの現状の認識とテロリズムの定義を必要とする。東西冷戦終焉後、テロリズムの定義そのものが大きく変化している。思想的、政治的、宗教的、民族的、地域的背景によるテロ活動が多様化し、また組織が分散化している。同時に、意図、目的、目標、手段も多種多様となっている。

そのようなテロ活動の一手段として、サイバーを利用したテロリズムの可能性が考えられる。サイバー上でのテロ行為は、テロリストにとり多くの優位性と効率性を備えている。これはネットワーク犯罪全般に共通することであるがネットワークの特性、すなわち時間的制約、資金的制約、物理的制約等からの開放、隠密性などは、テロリストに安全な位置からのより効果的な攻撃を可能にする手段と予測されている。また、サイバーテロリズムでは未組織グループ、あるいは複数の異なる背景を持つグループがネットワークで結びつき、共同テロが展開される可能性が高まることが予想される。

サイバーテロリズム、あるいはインフォメーション・ウォーフェア（IW、情報戦、あるいは情報戦争）という言葉が随所で用いられているが、その定義、概念は確立されていない。

サイバーテロリズムはネットワークを介して生産設備、社会機構等の機能に損害を与えるものであり、損害の現象は物理的領域で起こるものである。しかし、ネットワークを介しての攻撃は物理的攻撃と比べはるかに発見し難く、防御し難いものであり、現状では対策にも限界がある。

ネットワークを介しての攻撃ではITの知識のみならず、攻撃対象のシステム、設備、装置等に関する高度な専門知識を必要とするものである。度々ハッカーの行為とサイバーテロリズムを同等に論じられることがあるが、ネットワークへの侵入手法、手段に差異は少ないものの、能力、目的、意図は基本的に異なるものであり、ハッカーと同一視すべきではない。たとえハッカーにより大規模な障害が起こされたとしても、それをサイバーテロリズムと認識することはできない。

以下、国際会議におけるステファン・ブライアン博士のプレゼンテーションにおけるサイバーテロリズムに関する部分の要約を引用する。

『サイバーテロリズムとは、単に数名のコンピュータハッカーから攻撃を受ける場合よりも影響が大きく、広範囲にわたる問題である。事実、サイバーテロリズムは一種の情報戦争と定義づけられている⁹。クラス と表現している。情報戦争には3つのクラスがあり、サイバーテロリズムは第三のクラスに当てはまる。それは、産業、(単に国レベルでなく)世界規模の経済圏、国全体をターゲットにしたものであり、政治分野にまで影響の及ぶ戦争行為と定義される。

サイバーテロリズムは、第1に、技術に技術で対抗することであり、まったく新しいタイプの行為である。第2に、機密情報を巡る攻防であり、それを盗もうとする戦いである。どの政府機関にも、どの民間企業にも、保護したい情報があり、それが対象となる。第3に、情報をその所有者に不利になるように逆用することである。誰かから情報を盗めば、その情報を使って、情報の所有者を困らせることができる。第4に、敵にその技術や情報を使用できなくさせる戦いである。

攻撃の標的は、システムである。第1に、システムやデータの破壊、改ざんを狙う。第2に、データを不正閲覧またはコピーを狙う。第3には、システムリソースの不正使用を狙う。第4に、認定ユーザのサービス妨害を狙う。

国家安全保障上では、軍事機構や軍事統制の混乱が考えられる。これは、昔から情報戦争が繰り広げられている領域でもある。

第1に、彼らの目的は敵のコンピュータ・ネットワークに侵入することになる。第2に、情報の収集である。これは、きわめて価値の高い仕事である。第3に、科学技術の獲得。言い換えれば、技術を盗むことである。友好国、敵対国を含め多くの国が活動しているところである。第4に、偽情報の流布である。第5に、活動や業務の混乱を狙った働きであり、コソボ危機では米国は実際にユーゴスラビアのコンピュータ・システムを混乱させようと試みた。第6に、重要インフラを麻痺させる試みである。

テロリストの目的は次のとおりである。

第1に、大惨事を起こすこと。

第2に、常にテロリストの大義とテロリストのイデオロギーに注意を引きつけること。

第3に、敵を間断なく攻撃して悩ませ、威嚇すること。

第4に、死と破壊をもたらすこと。

サイバーテロリズムの脅威は増しつつある。外部からの敵意を持つ脅威が、より高度になりつつある。単なるハッカーの時代はもう終わり、われわれの

⁹ 国際会議のパネルディスカッションにおけるステファン・ブライアン博士のプレゼンテーションを参照。

相手はプロ級の敵である。好戦的国家が情報戦争やサイバーテロリズムのような活動により多くのリソースを注ぎ込んでいる。サイバーテロリズムのような活動の実施により多額の資金が投入されている』

サイバーテロリズムの対象としては、

1. システムの停止等が社会の混乱に結びつく公共性の高い施設
2. プラント等の運転が攪乱されることで危険な状態になる設備
3. 情報操作、脅迫を含め、ネットワークへの攻撃により社会秩序、信用秩序が攪乱される機構

があげられる。また、単一設備への攻撃では十分な効果が得られない場合には、複数設備、複数系統への同時多発的攻撃が考えられる。これらの攻撃準備は、相当の時間をかけて行われると予測され、ハッカーが試みるようなネットワークへの「侵入」ではなく、長時間ネットワークに「潜入」してネットワーク内を探索し準備することとなる。

ネットワーク上では瞬時に大規模、広範囲な障害を発生させられる可能性があり、特にサイバーテロリズム対策としては企業と法執行機関、捜査機関等の密接な協力が不可欠となつてこよう。従って、サイバーテロリズムは一企業で対処できるものでもなく、一国家で対応することも困難な場合があると考えられる。

あるネットワークの不十分なセキュリティが、ネットワーク全体に重大な被害を及ぼす可能性があり、一義的に各ネットワーク管理者は責任をもって十分なセキュリティ対策を講じることが不可欠である。

(2) 脅威分析

サイバーテロリズムの脅威は拡散しており、また攻撃対象の特定もますます困難となっている。

具体的な脅威例としては、敵性国家、思想宗教集団、独立運動集団、犯罪組織、圧力団体、不満分子などがある。

ネットワークを通じてのテロリストによる協力者のリクルートも容易となるため、組織内で不満、反感をもつ者などの内通者獲得が簡便に行われると認識すべきである。内通者にとり身分を明かされるなどのリスクが少なく、テロ組織へに参加、組み込みの認識も希薄なまま、自己欲求の達成という野心を持つことができる。

前述のごとく、ネットワークへの侵入が果たせたとしてもITの知識のみでは大きな損害を与えることは不可能に近い。攻撃対象の設備、全体システ

ム等の設計図段階からの専門知識が必要とされる。そのために、内部協力者あるいは離職者等の内部に精通した協力者のリクルートが十分考えられる。

脅威についてステファン・ブライアン博士は以下のような分類を試みている。

- 外部からの脅威か、内部からの脅威か（両方の場合もある）
- 敵意を持ったものかどうか（脅威はどれも敵意を持つものとは限らない）
- 構造的な脅威かどうか（構造的な脅威とは計画されたもののことである）

「内部からの、敵意を持たない、構造的でない」脅威は、例えば、だれかが不注意で社内ホストコンピュータシステムのサーバー上のデータをすべて消去してしまうといった場合が該当する。そんなつもりはなかったとしても、結果から見れば外部の敵意を持つ脅威によるものとほとんど同じことになる。

ピエテル・ファン・ディヒケン氏は企業の立場から脅威の性質と種類について、以下のように述べている。

『脅威が業務の状況にどう反映しているのか当社が目をつけているのは、次の点である。』

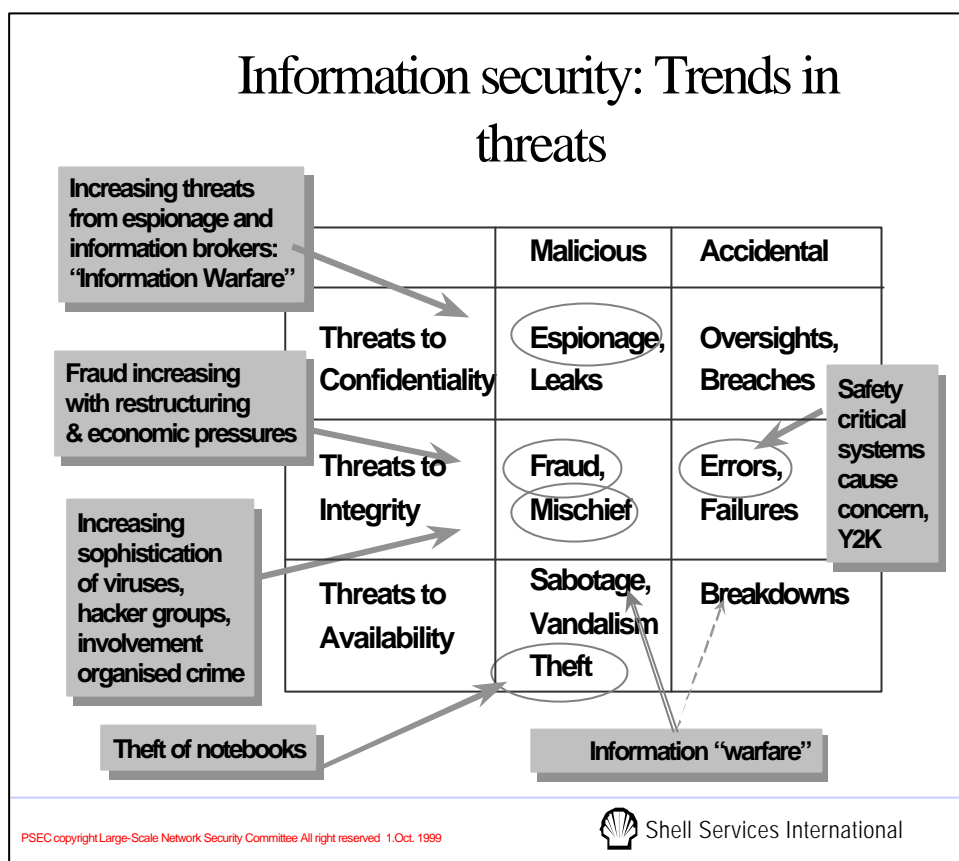
- 一般的に、不安定度と予想の困難度が増加している
- 情報に対する脅威が増し、困難な事業環境がそれに拍車をかけている
- 情報技術システムの悪用範囲が広がりつつある
- 組織犯罪、テロリスト、情報ブローカー、その他のグループのつながりが深まりつつある。情報ブローカーは産業スパイであり、企業相手に企業の秘密情報を売買する。当社はその脅威を十分認識し、それによって大きな被害を受けた経験もある。

次の図は、「悪意によるもの」と「偶発的なもの」を分け、もう一つの角度から、「機密保持への脅威」、「完全性への脅威」、「可用性への脅威」に分けたものである。（図表5）

この一部は、当社の属する業種に確実に特別な影響がある。特に、情報戦争タイプの脅威である。破壊行為が成功すれば、インフラが動かなくなり、顧客に提供しているサービスが大幅に停止することになる。

今日のハッカー集団に対する評価を集計すると、

- 高度に組織化されている



図表 5

- ビジネスとして行っており、面白半分でやっているのではない
- きわめて高性能なツールを持っている
- 組織犯罪、情報ブローカー、諜報機関などつながり、ハッカーを支援する諜報組織が多く存在する
- 自らを防衛する術も心得ている
- インターネットを使って攻撃の調整や情報交換を行っている』

3.1.3 国際協力の必要性

サイバーテロリズムは国際犯罪の可能性が非常に高い。つまり、サイバーテロリストが複数国に分散しネットワークを通じて活動し、または、外国からの、あるいは外国への攻撃が数カ国の国境をまたいで行われることが想定される。そのため、サイバーテロリズムの阻止、捜査、情報収集は国際間の協力が不可欠である。また、関係国間でのネットワーク監視協力体制、監視技術開発体制、監視情報交換体制の確立も必要と考えられているが、現状で

はその枠組みはでき上がっておらず各国相互の信頼関係の確立も十分に行われていない。

3.1.4 課題

(1) 専門家の不足

ネットワーク化が急速に発展する中で、情報セキュリティの専門家が不足している。

本来、IT 専門家とセキュリティ専門家は各々異なる専門分野である。セキュリティ自体はIT よりも長い歴史を持つ学問体系として成り立っており、その知識と経験をいかにIT セキュリティ、情報セキュリティに取り入れるかが課題である。双方を熟知している専門家は極端に少なく、情報セキュリティ発展の一つの障害ともなっている。効率的なセキュリティを確立し、システムの肥大化を避けるためにも専門家の育成が急務である。

また、情報セキュリティ・マネージメントを組織内で実施していくためには、「技術だけ、セキュリティ管理だけに依存するのではなく、第一線に教育のある人材を配備することも必要である」、「技術面では、アプリケーション、データ、インフラがある。プロセスの面では、手順、標準、成果の測定、会社の経営法がある。そして、人材面では、何をにおいても上級管理者の責任である」(ピエテル・ファン・ディヒケン氏の発言より)

(2) コミュニケーションギャップ

コミュニケーションギャップは、IT 担当者と、経営者を含めた他部門との間に存在すると考えられる。コンピュータ・ネットワークの専門用語、略語の使用は、構造、機能を把握していない人々にとってはコンピュータをブラックボックス化することに他ならない。しかしながら、セキュリティ対策は端末機器に接触する全ての人々が理解し、実行しなくてはならないものであり、また、トップ・マネージメントの主要な責務であるリスク・マネージメントを行ううえでも、コンピュータ・ネットワークのリスクを十分把握する必要がある。

全社的なセキュリティへの理解を深めるためには、IT 担当者あるいはセキュリティ担当者による教育啓発活動が不可欠であり、コミュニケーションギャップが起きないようにセキュリティを説明する努力を怠ってはならない。大

切なことは、自動車の安全運転の履行を促すことであり、エアバッグやABS装置の構造の説明ではない。

3.2 プラント・ネットワーク・セキュリティ運用ガイドラインの策定

前年度調査においては、既に通産省告示として出されている「情報システム安全対策基準」、「コンピュータ不正アクセス対策基準」、「コンピュータウイルス対策基準」、「システム監査基準」に対して、大規模プラント・ネットワーク・システムに適用できるようにするためには何を削除、追加すべきかを調査した。今回は、その調査結果に基づいて、対策基準を具体的に「プラント用セキュリティ運用ガイドライン」（別冊の資料編に収録）として策定した。

3.2.1 運用ガイドラインの策定

(1) 運用ガイドラインの策定の意義

中間報告書の第4章にも触れられているが、本委員会は、現状では制御系システムのセキュリティレベルに対する認識が企業間で異なるため、求められるレベルを示す客観的な基準が必要であると考えられた。

運用ガイドラインは、制御系システムにおけるコンピュータ不正アクセスによる被害の予防、早期発見及び拡大・再発防止のために、企業等の組織が実施すべき対策を取りまとめたものであるが、実際の適用に当たっては、本基準に沿って各企業等が自らの実情に応じた自主基準を策定することが望ましい。

(2) 運用ガイドラインの策定の方法

前回の調査における既存対策基準への追加の提案では、不正アクセス対策基準に対して多く出されている。そこで、この不正アクセス対策基準の追加項目の提案を今回の運用ガイドラインにおいては、どのように取り扱うべきか検討し、以下の方法によって運用ガイドラインを策定した。

(3) 不正アクセス対策基準の改訂

セキュリティ運用ガイドラインの策定を考える場合、昨年度の検討を基にするとプラント・ネットワークへの不正アクセス防止およびコンピュータ・ウイルスの侵入防止に係わる基準を策定すればよいものと思われる。検討の結果、以下のとおりとして策定した。

- ・ガイドラインの本文は「コンピュータ不正アクセス対策基準」をプラント・ネットワーク用に改訂することにより作成する。
- ・安全対策基準、ウィルス対策基準、システム監査基準についてはプラント・ネットワーク用に適用する場合の注意事項を記して参照する形とする。
- ・運用ガイドラインに含めない他の基準の参照は、従来の基準のように留意事項とせず、運用ガイドラインの一部として遵守を促すよう記述方法を工夫する。
- ・保守・リモートメンテナンスを行う事業者の基準を追加する。
- ・不正アクセス対策基準に含まれる「個人ユーザが留意する点」は、個人ユーザは、プラント・ネットワークと関係が皆無であるので、運用ガイドラインには盛り込まない。

以下に、策定した「プラント用セキュリティ運用ガイドライン」から、上述の要点を抜粋して示す。

< 参照すべき注意事項 >

他基準の参照

制御系システムのセキュリティを確保するため、本ガイドライン以外に以下に示す各規準も遵守することが望ましい。

1. コンピュータウイルス対策基準

コンピュータウイルス対策の実施については、「コンピュータウイルス対策基準」(平成7年7月7日付 通産省告示第429号)に準拠すること。

2. 情報システム安全対策基準

システム自体の安全対策実施については、以下の点を考慮の上「情報システム安全対策基準」(平成7年8月29日付 通産省告示第518号)を活用すること。

- (1) 電源設備: 制御系システムには災害時の停電対策としてバックアップ電源設備を設置すること。
- (2) 地震対策: 制御系システムは地震の際も極力停止しないよう考慮すること。
- (3) 設置環境: 制御系システムの運用に関する機器のための防水カバー - 常備は不要とする。
- (4) 災害対策: 制御系システムでは災害の際の遠隔地バックアップ機能は不要とする。

3. システム監査基準

システム監査の実施については、「システム監査基準」(平成8年1月30日付 通産省公報)を活用すること。なお活用にあたっては多くのプロセス制御システムが無人運転のオンライン・リアルタイム・システムであることを考慮の上、適用する項目の取捨選択を行うこと。

4. ソフトウェア管理ガイドライン

ソフトウェア管理の実施については、「ソフトウェア管理ガイドライン」(平成7年11月15日付 通産省公報)を活用すること。

< 追加した保守・リモートメンテナンスを行う事業者の基準 >

4. リモートメンテナンス事業者基準

(1) 管理体制の整備

リモートメンテナンス事業者の要員の業務範囲を明確にすること。
保守・開発用ドキュメント等の管理体制、管理基準を確立し、周知・徹底すること。
不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知・徹底すること。

(2) リモートメンテナンスユーザ管理

リモートメンテナンス事業者及びリモートメンテナンスユーザの責任範囲を明確にすること。
リモートメンテナンス事業者が提供できるセキュリティサービスを明示すること。
リモートメンテナンスユーザとの連絡体制を複数確立し、周知・徹底すること。
リモートメンテナンスユーザへの不正アクセスを監視できる仕組みを確立すること。
リモートメンテナンスの実施状況等を記録できる仕組みを確立すること。

(3) 情報管理

以下略

なお、運用ガイドラインの対象とするプラント・ネットワークを、中間報告の図 - 1 (システム構成モデル) を示す等の方法で明示する。

また、ウィルス対策基準は殆ど変更なしで適用できるものと思われる。

(4) 侵入経路別セキュリティ対策の運用ガイドラインへの適用

前年度調査では、セキュリティ侵犯を「何らかの経路からネットワークへ不正に侵入するか、侵入後機密を不正取得したりプログラムやデータを改ざん・破壊すること」と捉え、侵入経路別の対策を提案している。

この提案の内容には数多くの運用上の対策が含まれている。それらの侵入経路別対策と既存対策基準の項目との対応を整理し、新規に追加すべき事項を対策基準として追加することとした。

しかし、追加項目のかなりの部分が現状の不正アクセス対策基準に既にある項目で代替できるため、実際に追加する項目は3項目のみとしてよいことが確認された。(付表参照)

項目を追加しない場合には「セキュリティ・ポリシー」「無線ネットワーク」等の用語を運用ガイドラインの適当な項目へ追記して、前年度調査の提案に沿うようにした。

(5) セキュリティ対策を実施する者の定義の見直し

「セキュリティ対策を実施する者」(すなわち、「システムユーザ」、「システム管理者」、「リモートメンテナンス」)の定義については、大規模プラント・ネットワークに適用される運用ガイドラインとして、運用実態に則して見直した。

以下に、見直した定義を制定した「ガイドライン」から記す。

1. 制御系システムユーザ基準

制御系システムを利用する者(以下「**制御系システムユーザ**」とする。)が実施すべき対策についてまとめたもの。

2. 制御系システム管理者基準

制御系システムユーザの管理並びに**制御系システム**及びその構成要素の導入、維持、保守等の管理を行う者(以下「**制御系システム管理者**」とする。)が、実施すべき対策についてまとめたもの。

3. ハードウェア・ソフトウェア供給者基準

ハードウェア及びソフトウェア製品の開発、製造、販売等を行う者(以下「**ハードウェア・ソフトウェア供給者**」とする。)が、実施すべき対策についてまとめたもの。

4. リモートメンテナンス事業者基準

ネットワークを介して、**制御系システム**に対する**診断、修復等**を行う事業者(以下「**リモートメンテナンス事業者**」とする。)が、実施すべき対策についてまとめたもの。

5. ネットワークサービス事業者基準

ネットワークを利用して、情報サービス及びネットワーク接続サービスを提供する事業者(以下「**ネットワークサービス事業者**」とする。)が実施すべき対策についてまとめたもの。

大規模プラント・ネットワークでは、事業所間の通信及びリモートメンテナンスのための通信にネットワークサービス事業者が関わる可能性があるため、この基準を設けた。

(6) 用語の追加等

プラント・ネットワークの運用に携わる者が理解し易いよう、対象となるネットワークを図示し、また、「情報系システム」、「制御系システム」、「大規模プラント・ネットワーク」など、対象となるプラント・ネットワーク固有の用語の定義を追加した。

3.2.2 今後の課題

今回「コンピューター不正アクセス対策基準」を改訂することにより大規模プラント・ネットワークのセキュリティ対策を「プラント・ネットワーク・セキュリティ運用ガイドライン」として策定したが、これを公式に制定し、広く普及させる目的で、実際にプラント・ネットワークの管理、運用に携わる者が理解し易いよう、石油精製プラントなどの具体的なネットワーク例を示して運用ガイドラインの適用方法を示す解説書を作成することを今後の課題として提案する。

【別表1】 - 1

不正アクセス対策基準の追加項目(中間報告 参考資料4)の運用ガイドラインへの適用

中間報告の追加項目(案)		運用ガイドラインでの取扱い		備考
基準名・項目名	追加項目内容	基準名・項目名	番号	
1.システムユーザ基準 (3)コンピュータ管理	制御ネットワーク外部からの不正アクセスを防止するため、ファイアウォールの設置等適切な処置をとること。	2.システム管理者基準 (4)設備管理		
1.システムユーザ基準 (3)コンピュータ管理	制御系ネットワークを構成するルータ、ブリッジ等の通信機器への不正な書き込み、改ざんを防止する機能を取り入れること。	2.システム管理者基準 (3)情報管理		
1.システムユーザ基準 (3)コンピュータ管理	制御系ネットワークを構成する各機器のIPアドレス、ルータの Paket フィルタリング情報等の構成管理情報が制御系ネットワーク外へ不正に漏えいすることのないよう適切な処置をとること。	2.システム管理者基準 (3)情報管理		
1.システムユーザ基準 (3)コンピュータ管理	通信経路上で情報の改ざんが検出された場合は、システム管理者に通知する機能を設けること。	2.システム管理者基準 (3)情報管理		
1.システムユーザ基準 (3)コンピュータ管理	通信経路上で情報の改ざんが検出された場合は、プラント運転に不要なネットワークをクローズする機能を設けること。	2.システム管理者基準 (3)情報管理	新	プラント用特殊機能
2.システム管理者基準 (X)プラント運転情報管理	システム内への外部からのアクセス情報を管理する機能を設けること。	2.システム管理者基準 (3)情報管理	新	
2.システム管理者基準 (X)プラント運転情報管理	システム内の管理情報の変更は、指定(限定)された人のみが可能な機能を設けること。	2.システム管理者基準 (2)システムユーザ管理		
2.システム管理者基準 (X)プラント運転情報管理	外部からの侵入(アクセス)が発見された場合は、すみやかに接続の切り離しを行うとともに、管理者に連絡すること。	2.システム管理者基準 (6)事後対応	新	プラント用特殊機能
2.システム管理者基準 (X)プラント運転情報管理	システム内管理情報の改ざんが検出された場合は、システム管理者に連絡すること。	1.システムユーザ基準 (4)事後対応		
3.ネットワークサービス事業者基準 (1)管理体制の整備	ネットワーク内で不正アクセスや情報の漏えいを防止するための適切な対策をとること。	5.ネットワークサービス事業者基準 (2)ネットワークサービス管理		

中間報告の追加項目(案)		運用ガイドラインでの取扱い		備考
基準名・項目名	追加項目内容	基準名・項目名	番号	
4.ハードウェア・ソフトウェア供給者基準 (3)開発管理	制御系ネットワーク外部からの不正アクセスを防止するため、納入するシステムに対してファイアウォール設置等の適切な処置をとること。	3.ハードウェア・ソフトウェア供給者基準 (3)開発管理		
4.ハードウェア・ソフトウェア供給者基準 (3)開発管理	制御系ネットワークを構成する、ルータ、ブリッジ等の通信機器への不正な書き込み、改ざんを防止する機能を納入するシステムに取り入れること。	3.ハードウェア・ソフトウェア供給者基準 (3)開発管理		
4.ハードウェア・ソフトウェア供給者基準 (3)開発管理	制御系ネットワークを構成する各機器のIPアドレス、ルータのパケットフィルタリング情報等の構成管理情報が制御系ネットワーク外へ不正に漏れいすることのないよう納入するシステムに対して適切な処置をとること。	3.ハードウェア・ソフトウェア供給者基準 (3)開発管理		

【別表 2】

「3.4 侵入経路別のセキュリティ対策」と「運用ガイドライン」との対応

NO	侵入経路別のセキュリティ対策			運用ガイドライン			備考
	項番	項目名	テーマ名	項番	基準名	項目名	
1	3.4(1)	情報系との接続	セキュリティポリシー設定	2(1)	システム管理者基準	管理体系の整備	
2			最小サービスに限定	2(4)	システム管理者基準	設備管理	
3			アドレス漏洩防止	1(3)	システムユーザ基準	コンピュータ管理	
4			定期的に変更	1(1)	システムユーザ基準	パスワード及びユーザII管理	
5			接続機器限定	2(4)	システム管理者基準	設備管理	
6			ログ検査	2(5)	システム管理者基準	履歴管理	
7			不要なネットワークサービス削除	2(4)	システム管理者基準	設備管理	
8			OSのパケットルーティング制限	2(9)	システム管理者基準	プラント運転管理情報	新
9			ログの保全措置	2(5)	システム管理者基準	履歴管理	
10	3.4(2)	ダイヤルアップ	電話番号制限	2(2)	システム管理者基準	システムユーザ管理	
11			異なったパスワード	1(1)	システムユーザ基準	パスワード及びユーザII管理	
12			プロンプト変更	2(4)	システム管理者基準	システムユーザ管理	新
13			プロンプト情報の制限	2(4)	システム管理者基準	設備管理	新
14			誤入力時のレスポンス遅延	2(4)	システム管理者基準	設備管理	新
15	3.4(3)	無線ネット	別セグメント化	2(4)	システム管理者基準	設備管理	新
16			アドレス情報定期的変更	2(4)	システム管理者基準	設備管理	新
17			不使用時電源断	1(3)	システムユーザ基準	コンピュータ管理	
18	3.4(4)	計画、設計、建設時	入退出管理	3(2)	ハードウェア・ソフトウェア供給者基準	設備管理	
19			文書管理	3(3)	ハードウェア・ソフトウェア供給者基準	開閉管理	新
20			管理基準整備	3(3)	ハードウェア・ソフトウェア供給者基準	開閉管理	新
21			電子情報管理基準	3(3)	ハードウェア・ソフトウェア供給者基準	開閉管理	新
22			デフォルトパラメータの変更	3(3)	ハードウェア・ソフトウェア供給者基準	開閉管理	新
23			パスワード運用時変更	3(3)	ハードウェア・ソフトウェア供給者基準	開閉管理	新
24	3.4(5)	保守、メンテナンス	サービス提供者は信頼できる組織	4(1)	メンテナンス事業者基準	管理体制の整備	新
25			サービス提供者の入退出管理	4(4)	メンテナンス事業者基準	設備管理	
26			サービス提供者の文書管理	4(3)	メンテナンス事業者基準	情報管理	
27			サービス提供者のネットワークセキュリティ	4(4)	メンテナンス事業者基準	設備管理	
28			サービス提供者のシステム管理	4(4)	メンテナンス事業者基準	設備管理	
29			信頼できる保守要員	4(1)	メンテナンス事業者基準	管理体制の整備	新
30			保守要員教育	4(6)	メンテナンス事業者基準	情報収集及び教育	
31			保守要員管理監視	4(1)	メンテナンス事業者基準	管理体制の整備	
32			サービス提供者入退出管理	4(4)	メンテナンス事業者基準	設備管理	
33			サービス提供者文書管理	4(3)	メンテナンス事業者基準	情報管理	
34			サービス提供者顧客情報管理	4(3)	メンテナンス事業者基準	情報管理	
35			サービス提供者開閉管理	4(3)	メンテナンス事業者基準	情報管理	新
36			サービス提供者要員管理	4(1)	メンテナンス事業者基準	管理体制の整備	新
37			セキュリティ教育	4(6)	メンテナンス事業者基準	情報収集及び教育	
38			ウイルス対策				*1
39			監視と監査	4(7)	メンテナンス事業者基準	監査	
40			セキュリティポリシー	2(1)	システム管理者基準	管理体制の整備	
41			対象サービスと提供方式の選択	2(4)	システム管理者基準	事後対応	
42			監視と監査	2(4)	システム管理者基準	事後対応	新
43			独立環境	4(4)	メンテナンス事業者基準	設備管理	
44			情報の秘匿	4(3)	メンテナンス事業者基準	情報管理	
45	3.4(6)	ウイルス対策	ウイルス対策				*1
46	3.4(7)	ソーシャルエンジニアリング対策	パスワード管理	1(1)	システムユーザ基準	パスワード及びユーザII管理	
47			教育	1(5)	システムユーザ基準	教育及び情報収集	
48			罰則規定	1(2)	システムユーザ基準	情報管理	新
49			外部要員管理	2(4)	システム管理者基準	設備管理	
50			監査	1(6)	システムユーザ基準	監査	

* 1 : 「コンピュータウイルス対策基準」

第4章 技術的事項の報告

4.1 セキュリティ技術開発

現在プラントで使用されているDCSの多くは、メーカー独自のOSが採用されているか、また制御系システム自体が情報系システムから切り離されているか、或いはメーカー独自のプロトコルによって接続されている。このため外部ネットワークから侵入される脅威は低い。従って現存の制御系システムにおいてはネットワークセキュリティ対策を取る必要性が低く、セキュリティ技術が殆ど導入されていないのが実状である。しかし今後DCSのオープン化、ネットワーク化の流れから、情報セキュリティ技術の導入の必要性が高まることは自明の理である。これ等セキュリティ技術の導入に関して、中間報告書においては次の二つの視点から提案がなされている。

1. 現在利用可能な技術を用いて実施すべきセキュリティ対策
2. 新しい防止技術の研究開発

これら二つの提案に対して、実際にプラントに適用する事を前提として双方合わせて再度技術的検討を行い、開発が必要な技術テーマを定義し、その機能概要を定めた。

4.1.1 中間報告書で提案された対策の再検討

(1) 技術的再検討と掘り下げ

中間報告書において「現在利用可能な技術」とした技術については、実際に制御系システムに適用されている例は少ない。これ等の技術を制御系システムに採用するに当たっては適用性、有効性、可用性の観点から再吟味することが必要である。また必ずしも一個のハードウェア/ソフトウェア製品によって具現化出来ている訳ではないので、制御系システム適用に関しては現製品の機能形態に縛られることはなく、再度「あるべき姿」から見直す必要がある。従って、「現在利用可能な技術」に関しても「開発テーマの選定」の候補としてリストに加えることにする。

詳細は中間報告書3.4 進入経路別のセキュリティ対策を参照されたい。

(2) 研究開発すべき技術について

中間報告書においては、防止技術の研究開発は経済性を含めて検討することが必要、との注記付きで以下のテーマを提案している。

- ・制御系システムへの認証技術の適用
- ・高速暗号化技術の開発と実証

- ・セキュリティ対策を施したDCSの開発検討
- ・疑似アタックの実験

指摘された事項は、情報系システムにおいて既に開発されている技術の制御系システムにおける適用、言い換えれば既存ビジネス系向けセキュリティ製品のプラント専用版の開発と実証である。

詳細は中間報告書4.3.防止技術の研究開発を参照されたい。

4.1.2 開発テーマの選定作業

(1) 選定手順

開発テーマの選定に当たりその手順を検討し、以下の順序に従うことにした。

- ・ 中間報告書で取り上げられている対策を、技術的対策と非技術的対策に分類する。
- ・ 技術的対策については、別途技術の体系化（下表参照）を行い、それによって分類する。
- ・ 非技術的対策については、「運用」と「その他」に分類する。
- ・ 中間報告書で取り上げられていない技術的対策の有無を確認し、必要があれば追加する。

【技術の体系化】

- * 侵入されたことを検知する技術
 - ・ 自動検知
 - 侵入検知
 - データ改変検知、ログ記録
 - 異常プログラム検知、ウイルス検知
- * 侵入を防止する技術
 - ・ ファイアウォール
 - 設計（プラント専用） 設定方法
 - ・ 通信プロトコル
 - SSL、リモート保守（無線）
 - ・ 認証
 - 機器認証
 - 利用者認証
 - プロセス認証
 - ・ 暗号化
 - 高速暗号化
 - 制御系への適用（タイミングなど）
- * その他の技術
 - ・ セキュアDCS
 - ・ 自動設計・検査
 - ・ 追跡・迎撃
 - ・ アクセス管理

(2) 選定結果

以上の手順によって整理された対策項目が次表である。

なお、取るべき対策各項目欄は中間報告書における小項目に対応している。
開発テーマ（候補）の選別結果（1/3）

中間報告書 3.4. 侵入経路別のセキュリティ対策	中間報告書に書かれている 取るべき対策	技術的対策	非技術的対策
(1) 情報系との接続	セキュリティポリシー設定		その他
	ファイアウォール設置	ファイアウォール	
	最小サービスに限定		運用
	アドレス情報漏洩防止		運用
	定期的にパスワード変更		運用
	ワンタイムパスワード	認証	
	接続機器限定		運用
	ログ検査		運用
	不要なネットワークサービス解除		運用
	OSのパケットルーティング無効化		運用
	ログの保全措置		運用
	暗号化	暗号化	
	認証システム導入	認証	
	通信機器の改ざん防止	ファイアウォール	
	不正侵入検知ツール実装	自動検知	
	ネット上の情報改ざん検知	自動検知	
	ファイアウォールの異常検知	ファイアウォール	
ルータでのルーティング制限	ファイアウォール		
(2) ダイアルアップ接続	電話番号制限		運用
	機器のパスワード認証	認証	
	リモートアクセスサーバ設置	認証	
	CHAP/PAPパスワード認証	認証	
	LANとは異なったパスワード		運用
	プロンプト変更		運用
	プロンプト情報の制限		運用
	誤入力時のレスポンス遅延		運用
(3) 無線ネットワーク	別セグメント		その他
	暗号パケット	暗号化	
	アドレス情報定期的変更		運用
	ファイアウォール利用	ファイアウォール	
	不使用時電源断		運用
(4) 計画、設計、建設時	入退出管理		運用
	文書管理		運用
	管理基準整備		その他
	電子情報管理基準		その他
	電子情報の認証	認証	
	デフォルトパラメータの変更		運用
	不正、不要プログラムのチェック	異常プログラム検知	
	ソフトウェア正当性チェック	異常プログラム検知	
	パスワード運用時変更		運用
	コールバックセキュリティ機器	通信プロトコル	

現時点での開発テーマ（候補）の選別結果（2/3）

中間報告書 3.4. 侵入経路別のセキュリティ対策	取るべき対策	技術的対策	非技術的対策
(5) 保守、リモートメンテナ /ベンダ	サービス提供者は信頼出来る組織		その他
	サービス提供者の入退出管理		運用
	サービス提供者の文書管理		運用
	サービス提供者のネットワーク セキュリティ		その他
	サービス提供者のシステム管理		運用
	信頼出来る保守要員		その他
	サービス提供者入退出管理		運用
	サービス提供者文書管理		運用
	サービス提供者顧客情報管理		運用
	サービス提供者開発管理		運用
	サービス提供者要員管理		運用
	セキュリティ教育		その他
	ウイルス対策		その他
	監視と監査		その他
保守、リモートメンテナ /ユーザ	セキュリティポリシー		その他
	対象サービスと提供方式の選定		その他
	監視と監査		その他
ベンダ/セキュリティ機能	要員の識別と承認	認証	
	接続時の認証	認証	
	コマンド/アクセス制限	アクセス管理	
	独立環境		その他
	情報の秘匿		運用
	不正操作ミスの監視と検知	自動検知	
(6) ウイルス対策	ウイルス対策		その他
(7) ソーシャルエンジニア リング対策	パスワード管理		運用
	利用者、機器の認証	認証	
	教育		その他
	罰則規定		その他
	外部要員管理		運用
	監査		その他

現時点での開発テーマ（候補）の選別結果（3/3）

中間報告書 4.3. 防止技術の研究開発	研究開発テーマ	技術体系
(1) 認証技術の適用	プラント専用ファイアウォール	ファイアウォール
	指紋による認証システム	認証
(2) 高速暗号化技術の開発と実証	暗号化	高速暗号化技術
	リアルタイム暗号/複合の実証	暗号化
(3) セキュアなDCSの開発	高機能化とオープン化に対応した 機能分化	セキュアDCS
	パラメータの変更履歴ログ取得	自動検知
(4) 擬似アタックの実験	セキュリティ・ホールのチェック	(総合)

その他	研究開発テーマ	技術体系
中間報告書で取り上げられていない技術的対策にかかわる研究開発テーマ	データへの電子透かし	認証
	ファイル暗号化	暗号化
	ファイアウォールの設定手法 追跡・迎撃	ファイアウォール 追跡・迎撃
	I/O複線化 フィールドバスのセキュリティ	セキュアOS (総合)

4.1.3 選定作業中に判明した事

(1) 現在利用可能とした技術について

現在利用可能とした技術が有効であるか、または今後研究開発が必要か判断作業を行う段階で以下のことが判明した。

上記「技術的対策」は製品/機能を具体的に明示している訳では無い。従って現在利用可能な製品でも、個別製品/機能毎に制御系システムへの適用性、有効性、可用性が異なるので、これらの製品/機能に関して再度評価しなければ「現在利用可能な技術」が「制御系システム」に対してそのまま利用可能であるか否か判断できない。言い換えれば、「現在利用可能な技術」とした技術であっても、今後の研究開発の必要性が高い技術であるケースがあり得る。

また、それらの製品の制御系システムへの適用に際しては、情報系システムへの適用とは異なる運用上の留意点が存在する場合があります。

(2) 研究開発すべきとした技術について

中間報告書において研究開発すべきとした技術は4.1.1(2)のお

りであり、開発テーマとしてそのまま対象になると判断できる。しかしこれらは4.1.1(2)に記述した様に、前項の「現在利用可能とした技術」と極めて類似している。

従って開発テーマとしては、現在利用可能技術と研究開発すべき技術、双方を対象として検討することとした。

4.1.4 テーマ選定結果

以上の検討作業により、既存のセキュリティ製品の変更(「現在利用可能な技術による製品」) および新規開発機能テーマとして以下を選定した。

セキュリティ技術	開発対象機能
侵入検知	センサー機能 (通信データ解析、 データ解析のためのログ、 アラーム、 マネージャとの通信)
	マネージャ機能 (ユーザーインターフェース、 検知パターン設定・管理、 侵入検知の通知・ログ、 センサーとの通信、 レポート生成)
ログ記録	D C S のログ記録・解析機能
ファイアウォール	制御系システム専用のファイアウォール (アクセス制御ルールの設定、 通信パケットのリレー、 パケットのブロック、 イベントのログ機能)
認証	制御LAN上の認証 (利用者および利用機器組み合わせ認証、 アクセス権限コントロール)
	制御系情報LAN上の認証 (制御データアクセスクライアントの認証)
暗号化	暗号技術評価用ソフトウェア
検査	制御ファイルアクセス権検査機能
	ネットワークポート検査機能
	機器アクセス権検査機能
	常駐プログラム制御権検査機能
	プログラム制御権検査機能
	パスワード検査機能
	セキュリティホール検査機能

4.1.5 まとめ

以上のように機能要件定義を行った後、コンソーシアムを組んで別途開発作業を開始した。テーマとしては：

- ・制御系システム専用のアクセス制御機能
- ・制御系システムのセキュリティ検査機能
- ・分散制御システム（DCS）のログ記録機能
- ・制御系システム専用の認証機能
- ・制御系情報LAN上での侵入検知機能
- ・「リモートアクセス環境でのセキュリティ」の評価機能
- ・統合試験機能
- ・「高速暗号技術」の評価機能
- ・実証実験（統合アタック実験）実施

を選定した。開発作業は各社分担で行い、最終的に評価のための統合アタック実験を行った。

統合アタック実験により、今回開発を行った機能の有効性は十分に確認できた。今後は更に、DCSに限定せず制御系システム全体としてのセキュリティ機能の検討、セキュリティ機能の全体の統合化、実装を前提とした再検討などを考慮した、製品化に向けた設計が必要であり、来年度以降の課題として残されている。

< 参考 > 開発作業および開発技術の有効性等に関する検証について

前述の様に、開発作業は以上の検討結果に従い、別プロジェクトとして作業が行われている。各開発機能の概要はそちらを参照されたい。

「大規模プラントのネットワーク・セキュリティ技術開発 / 実証実験
技術開発コンソーシアム公開報告書」 第一分冊 仮称

また中間報告書においてアタック実験の必要性が提案されている。これは今回のテーマ選定作業が机上作業によるものであるのに対し、現制御システムの脆弱性を実際に検証し、その結果として開発テーマ選定作業を行う事によりテーマの妥当性をより高めようと言う意味を持っている。

更に技術開発の最終フェーズとして、開発技術の制御系システムへの適用性、有効性、可用性の吟味を行い、更に追加開発すべき機能が無いか洗い出すと共に、適用上の留意点などを明確化することが必要である。従って技術開発後のアタック実験も必要不可欠であると考えられる。

この方針に従って以下三回のアタック実験が行われ、以下の報告書が別途作成されている。必要に応じて参照されたい。

- ・現DCS（カスタムOS）の疑似アタック実験
「石油プラントのネットワーク安全性検証実験」
- ・新世代DCS（UNIX，Windows / NT）の疑似アタック実験
「大規模プラントのネットワーク・セキュリティ技術開発 / 実証実験
安全性検証実験報告書」
- ・新規開発機能組み込み制御系システムに対するアタック実験
「大規模プラントのネットワーク・セキュリティ技術開発 / 実証実験
技術開発コンソーシアム公開報告書」 第二分冊 仮称

4.2 リスク分析手法

4.2.1 問題意識

大規模プラントネットワークに対する外部よりの脅威に対して、プラント設計者並びに運用者が事前にそのリスクを定量的に把握すると共に有効な対応策を施すことは、オープンシステム¹⁰採用の利益を享受するために当然払わねばならない代償である。

イントラネットを構成する目的でプラントネットワークをインターネットに接続した場合、理論的にはインターネットに接続された全てのコンピュータ（PCを含む）とそのユーザが潜在的脅威の対象となり得る。しかしながら、この想定に対応することは非現実的であり、どのような手法を採るにしても、リスク分析を行うには以下を特定する必要がある。

- ・ 対象システム範囲
- ・ 対象リスク
- ・ 実施時期

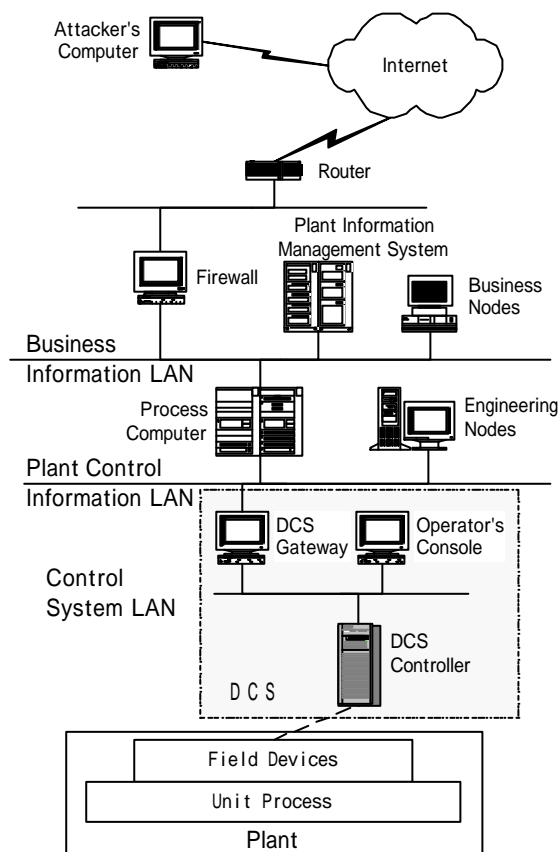


図4-2-1 概略プラントネットワーク

¹⁰ インターネット、オープンプロトコル、市販機器、市販ソフトなど

(1) 対象システム範囲の決定

対象システムの外縁を、インターネットとの接点である“ ルータへの侵入 ”とすることに異存がないであろう。ルータ以下どこまでをリスク分析対象とするかに関する検討図を図 4 - 2 - 2 に示す。ここでは、外縁のルータに対するアタックを想定し、アタッカーが図 4 - 2 - 1 に配されているセキュリティチェック機構を突破し、クリティカル情報に到達した場合のプラントへの影響を示している。

この図では、左から右へ行くほど時間が経過し、下から上に行くほどリスクが増加しており、C1(Fail in Access Control), C2(Intrude to Network), D2(Get Higher User ID), E3(Intrude to DCS)でセキュリティチェック機構が突破されている。しかしながら、プラントに当初から設置されている保安機構¹¹の作動により、ノード D6(Normal Operation with Isolated DCS)、E6(Normal Shutdown triggered by DCS Malfunction)あるいは F6(Normal Shutdown triggered by Interlock)としてプラントは正常に停止している。プ

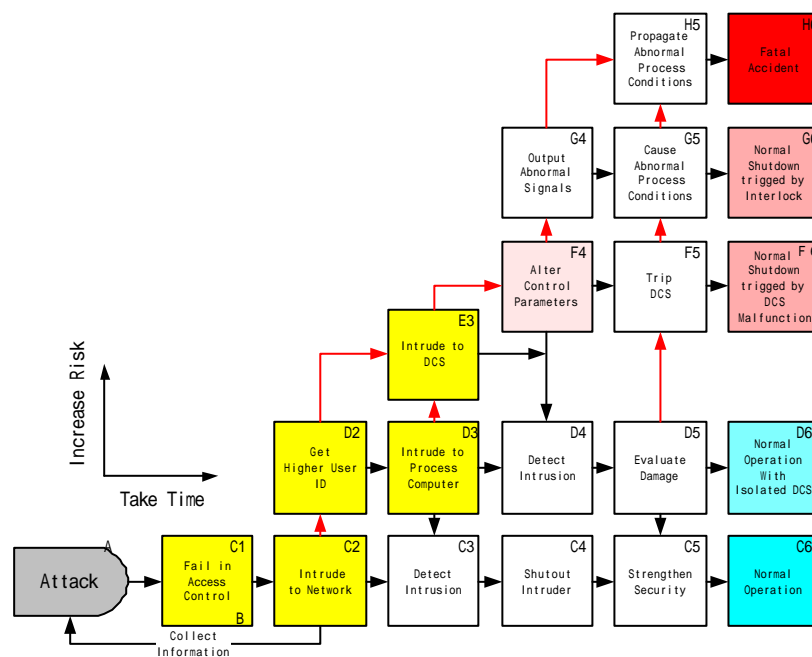


図 4 - 2 - 2 プラントにおけるセキュリティ・リスクの構造

¹¹ これらインターロック等の保安機構はプラント制御系とは別システムをなしており、阪神淡路大震災の際にもプラント災害を未然に防ぎ、その役割を実証している。

ラントが真に異常事態に陥るのは、ノード H6(Fatal Accident)に到達した場合に限られるており、H6 に至る過程における最終セキュリティチェック機構は E3(Intrude to DCS)である。したがって、その破局は F4(Alter Control Parameters) を引き起こす可能性が高く、ノード H6 に至る最短ルートであることが理解される。このため、リスク分析対象の内縁を“DCS への侵入”に置くことが妥当であると考える。

(2) 対象リスクの決定

対象とする最終リスクは、図 4 - 2 - 2 の E3(Intrude to DCS)とそれに伴う F4(Alter Control Parameters)である。このイベント発生に至る過程で生じるリスクとその対応策の記述方法は、採用するリスク分析手法に大きく依存する。これまで、リスク分析対象へのアプローチとして次の 2 通りが考案されてきた。

A) 定性的分析手法

機器に精通したエンジニアによる定性的なリスク分析を主眼とした手法であり、以下の 3 つに代表される。

Preliminary Risk Analysis (PRA)

Hazard and Operability studies (HAZOP)

Failure Mode and Effects Analysis (FMEA/FMECA)

B) ツリーベース分析手法

アクシデントのシナリオをモデル化することで異常事象に至るカットセットの発見に使用される手法であり、以下の 2 つが代表的な手法である。

Fault Tree Analysis (FTA)

Event Tree Analysis (ETA)

上記手法の応用(時間経過の考慮、FTA と ETA のとして、以下の手法がある。

Dynamic Event Tree Analysis Method (DETAM)

Cause-Consequence Analysis (CCA)

したがって、定性的分析手法並びにツリーベース分析手法からそれぞれ 1 手法を選定することで、発生しうるリスクの概要を把握することが可能であると考えられる。

(3) 実施時期の決定

プラント本体に対する保全処置は、プラント・セーフティ・エンジニアリングとして対応技術が確立されており、プラントライフサイクル（計画、設計、建設、運用フェーズ）にあわせた具体的な安全性分析がおこなわれている。同様に、プラントネットワークに対してもライフサイクルに対応したリスク分析手法が求められる。

ここで、プラント本体とプラントネットワークにおけるライフサイクルの違いは、

- ・ 本体は耐用年数が長く、高価であり、その不良が直接経営並びに安全に影響するため、計画・設計フェーズにおいて十分な分析と対応策検討が求められるのに比べ、プラントネットワークはハードウェアの技術変化が早く、利用技術も多様化する傾向にあり当初の計画・設計思想が急速に陳腐化するため、計画・設計フェーズにおける分析と対応策検討に比重をかけにくい点
- ・ 本体側は建設されるとほとんどハードウェア（プロセス構成、プロセス機器、制御装置等）並びにソフトウェア（オペレータ、操作・制御・運用方案等）がほとんど変化しないのに比べ、プラントネットワークはネットワーク上のハードウェア（ネットワーク構成、PC、ネットワークデバイス等）並びにソフトウェア（PC 上のアプリケーション、OS、使用者等）が変化するのが常態である点

にある。したがって、リスク分析手法としては計画・設計フェーズのみならず、運用フェーズにおいても統一的に使用できる手法であることが望ましい。

4.2.2 検討内容

上記の問題意識に基づき、次の2テーマを中心に検討を行なった。

テーマ1： セキュリティ・エンジニアリングのフレームワーク
プラント・ライフサイクルに則したリスク分析の位置付としその課題の検討を行った。

テーマ2： プラントネットワークに対するリスク分析手法
定性的アプローチとツリーベース分析手法から HAZOP と FTA/ETA を選択し、プラント・ネットワークにおけるリスク分析への適用性検討を行った。

HAZOP を応用した分析手法の検討

ステータス：概念設計フェーズまで実施

FTA/ETA を応用した分析手法の検討

ステータス：プロトタイプ作成まで実施

4.2.3 検討結果

プラント本体に対して適用されている HAZOP 並びに FTA/ETA をそのままプラントネットワークに適用することは、以下の制約から難しいものと考えられる。

HAZOP：専門家の知識への依存

- ・適切なガイドワードの選択
- ・トラブルとその影響の想定
- ・効果的な対応策の選択

FTA/ETA：動的な変化に対する適用性の欠如

- ・物理構造の変化によるダイナミクス
- ・論理構造の変化によるダイナミクス
- ・状態遷移によるダイナミクス

このため、本検討では既存の HAZOP 並びに FTA/ETA そのものを適用するわけではなく、これらの手法を拡張ないしは手法をアナロジーすることで上記制約を解消すること検討した。

(1) HAZOP の適用

概念設計の結果、以下の機能を有する必要があることが判明した。

- a) ネットワーク構造を定義する CAD 機能
- b) ネットワークトポロジーの監視機能
- c) ネットワーク機器の機能表現
- d) ネットワークトポロジーの分析機能
- e) HAZOP 手法によるリスク分析機能

詳細に関しては添付を参照願いたい。なお、本手法の全体像を図 4 - 2 - 3 に示す。

ここでは特に、本手法の実装上重要である d)並びに e)の 2 点に関する概念設計の結果を以下に示す。

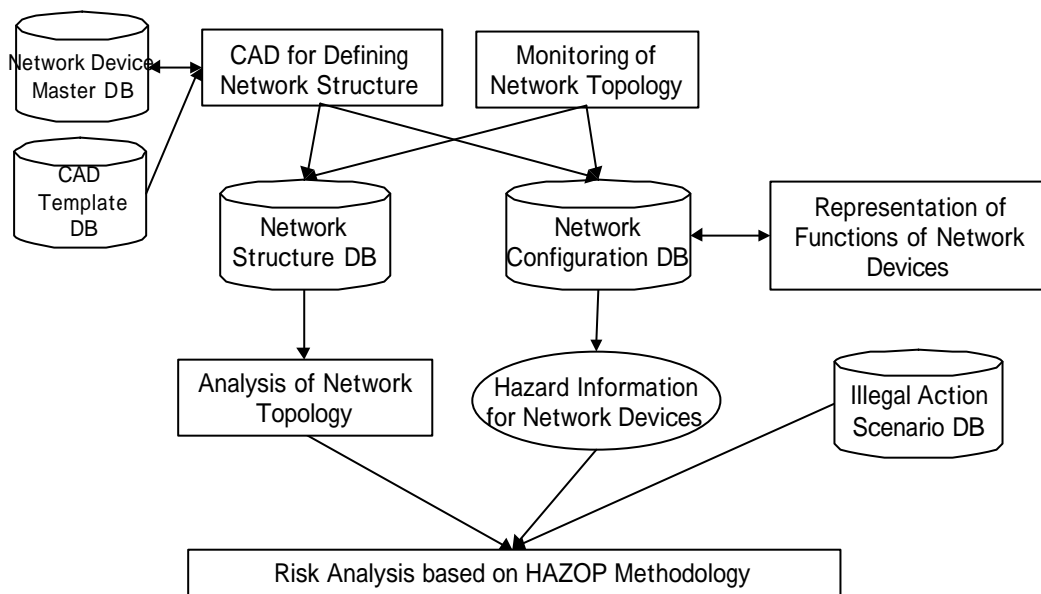
A) ネットワークトポロジーの分析機能

本機能は、次の 2 点を中心として実装される必要がある。

出) 指定した 2 つのネットワーク機器間における全ての物理的リンクの抽出

- ・ インターネット経由
- ・ 公衆回線経由
- ・ 社内 LAN 経由
- ・ プロセスコンピュータ経由
- ・ DCS 経由

出) 指定した 2 つのネットワーク機器間におけるデータフロー方向の抽出



B) HAZOP 手法によるリスク分析機能
本機能は、次の 2 点を中心として実装される必要がある。

-) 選択したシナリオの妥当性評価
 - ・ 違法行為シナリオの特定
 - ・ 違法行為に関わるネットワーク機器におけるハザード情報の収集
 - ・ 違法行為に関わるネットワーク機器におけるコンフィギュレーション情報の収集
-) 評価結果のレポート機能
 - ・ ネットワーク機器の推奨コンフィギュレーションの提示
 - ・ ネットワーク全体の評価レポート
 - ・ 各ネットワーク機器に対する評価レポート

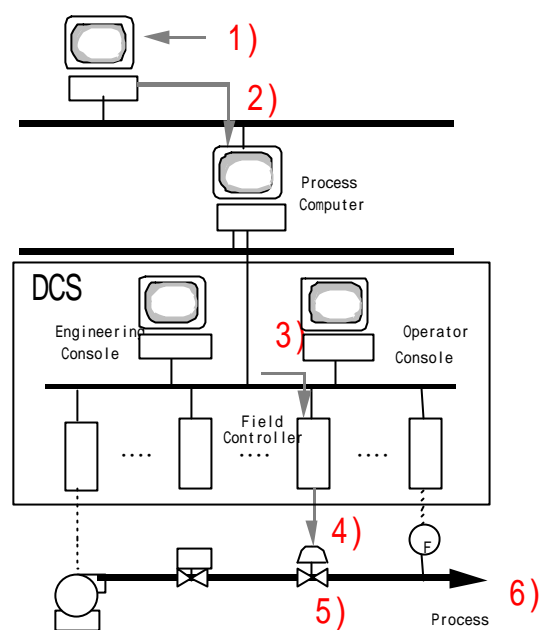


図 4 - 2 - 4 検討シナリオ

(2) FTA/ETA の適用

FTA/ETA 手法を適用する上で、違法アクセスからプラント本体の異常に至るシナリオとして、図 4 - 2 - 4 に示す次のステップを想定した。

- ステップ 1) ネットワーク上の PC へのアクセス Access to the Network PC.
- ステップ 2) DCS 機能を変更できるコンピュータへのログイン
- ステップ 3) DCS 機能を変更するコマンドの実行
- ステップ 4) 有害な制御シグナルの出力
- ステップ 5) 制御機器の誤作動.
- ステップ 6) プロセス異常の発生

このシナリオは、2 つのシステム、プラントネットワークとプラント本体に跨っている。FTA/ETA ではトップ事象からツリー構造を構成していくため、図 4 - 2 - 5 に示す 2 ステップ・アプローチで FTA/ETA を適用することとなる。

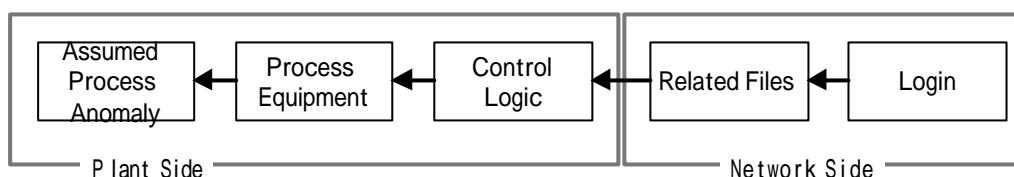


図 4 - 2 - 5 2ステップアプローチによる FTA/ETA の適用

第 1 ステップ:プラント側 FTA

トップ事象= 想定プロセス異常

ボトム事象= 制御ロジック内の制御情報

第 2 ステップ:ネットワーク側 FTA

トップ事象=制御ロジック・ファイル内の当該制御情報

ボトム事象= ネットワーク上のとあるコンピュータへの不正ログイン

A) プラント側 FTA

プラント側ハードウェアに対する FTA は確立された技術であり、多くの研究が発表されている。本検討では、ネットワーク側との接合を行う必要がある。このため、プラント側ハードウェア（特に制御機器）と制御ロジック並びに制御ロジックと制御ロジックが格納されているファイルまでボトム事象を拡張しており、調査した限りこのような適用例は発表されていない。しかしながら、FTA/ETA 手法を拡張する必要は認められず、適用範囲の拡張であると考えることが出来る。

B) ネットワーク側 FTA

ネットワーク側に FTA 手法を適用する上で核となる、経路の抽出並びに認証プロセスのモデル化に関して概説する。

）経路抽出

図 4 - 2 - 6 にある次の 2 つの経路を自動的に抽出することで、物理構造の動的な変化に対する適用性を高めている。

a) ログイン経路

ユーザ並びにホスト情報等を利用し、如何に目標マシンに到達するか。

b) ファイルアクセス経路

関連するファイル並びにコマンド等に如何にして到達し、どのように内容を変更するか。

）認証プロセスのモデル化

オペレーティングシステム (OS) 内で行われている認証プロセスを统一的に記述することで、論理構造の動的な変化に対する適用性を高めている。

図 4 - 2 - 6 経路情報の抽出

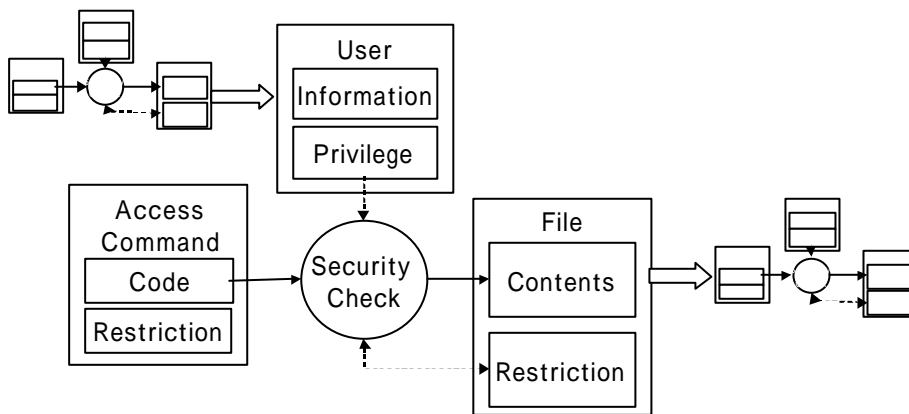
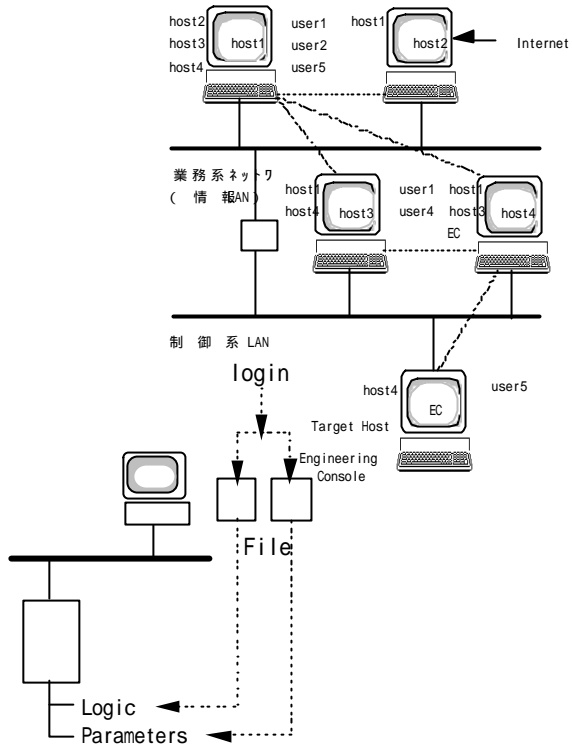


図 4 - 2 - 7 セキュリティチェック構造モデル

ほとんど全ての OS では、デバイス、コマンド、データ等のコンピュータ資源を、概念上ファイルとして管理している。このファイルに対するアクションには、常に OS のセキュリティ管理機構が関与してくる。この関与構造

をモデル化することで、どのようなアクション（コマンドの実行）であろうとその過程を FT に反映させることを可能としている。図 4 - 2 - 7 で示すモデルでは、コマンドの実態はコードと使用制約（許可）、ユーザはユーザ情報と特権、ファイルは内容と使用制約（許可）で構成されている。更に、セキュリティチェックをパスしアクセスされたファイルは、その実態がコマンドやユーザとして識別されており、再帰的に本モデルが適用されることが理解される。

以上 2 点の組み合わせから、ネットワーク側 FT は ET+FT 構成をとって、図 4 - 2 - 8 に示すごとくプラント側 FT と接合される。なお、詳細に関しては添付資料を参照願いたい。

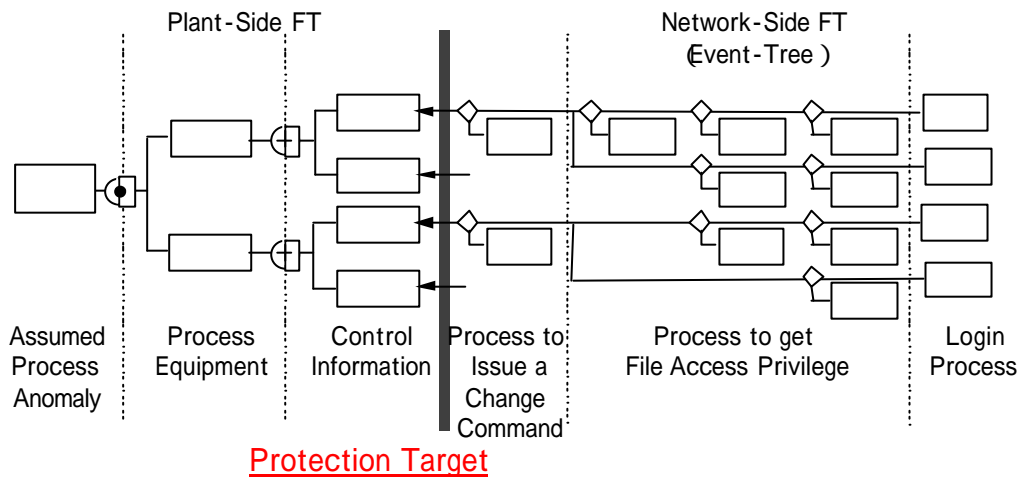
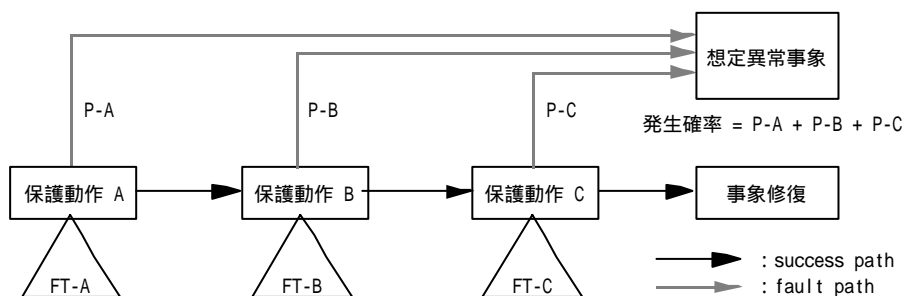


図 4 - 2 - 8 プラント側 FT とネットワーク側 FT の接合

なお、ET+FT 構造とは、以下のように保護動作をトップ事象とした FT とその保護動作のシーケンスを ET として表現したものである。



また、FTA/ETA の適用検討は、プロトタイプシステム開発まで進められている。ここでは、プロトタイププログラム実行時の画面ハードコピーの一部を次頁以降に示す。

図 4 - 2 - 9 に機能検証に用いたプラントモデル、DCS 上の制御ロジック図並びにネットワーク図を示す。プロトタイプシステムでは、これらの機能をコンピュータ上でシミュレーションを行うことによって、実際のプラントを模擬している。

図 4 - 2 - 10 にセキュリティチェック構造モデル例として UNIX 上の su コマンドを示す。

図 4 - 2 - 11 にプラントモデル上で発生し得る異常として出口圧力制御異常を指定することで自動作成されたプラント側 FT を示す。

図 4 - 2 - 12 にプラント側 FT のボトム事象となった制御パラメータの改変に関わるネットワーク側 FT を自動生成した途中経過を示す。最終的に生成されたネットワーク側 FT は侵入可能な全ての経路とそこで発生するセキュリティ異常を図示している。

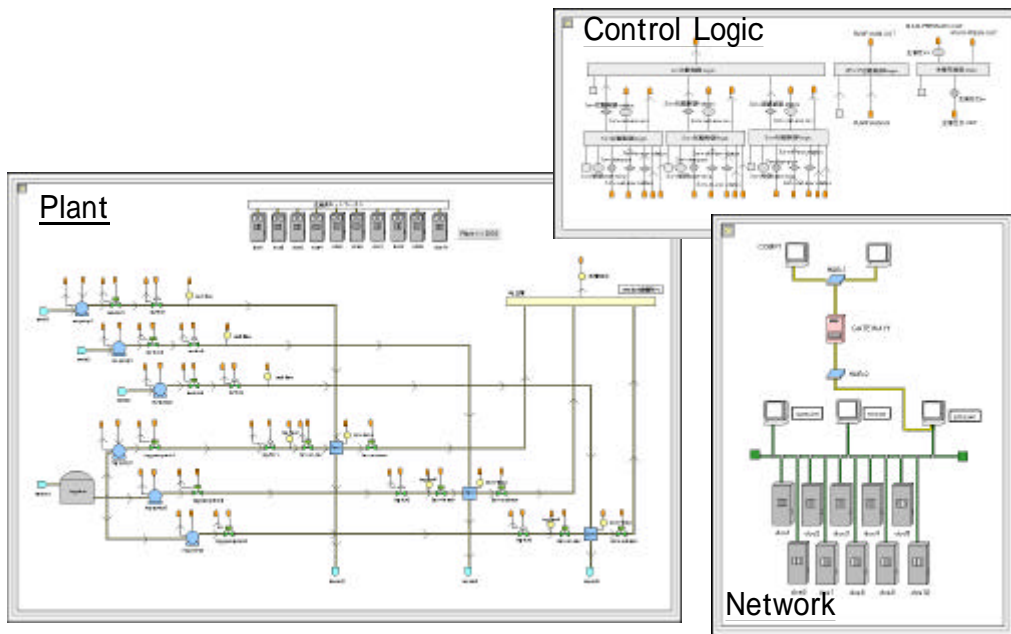


図 4 - 2 - 9 FTA プロトタイププログラムにおける機能検証用プラント、制御ロジック並びにプラントネットワーク

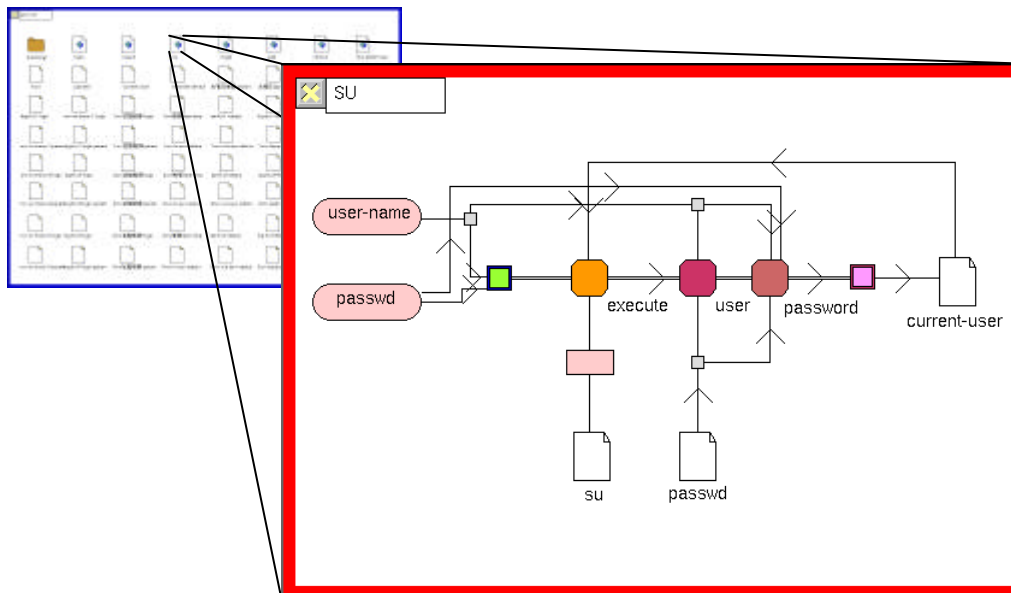


図 4 - 2 - 10 セキュリティチェック構造モデル (例：UNIX 上の su コマンド)

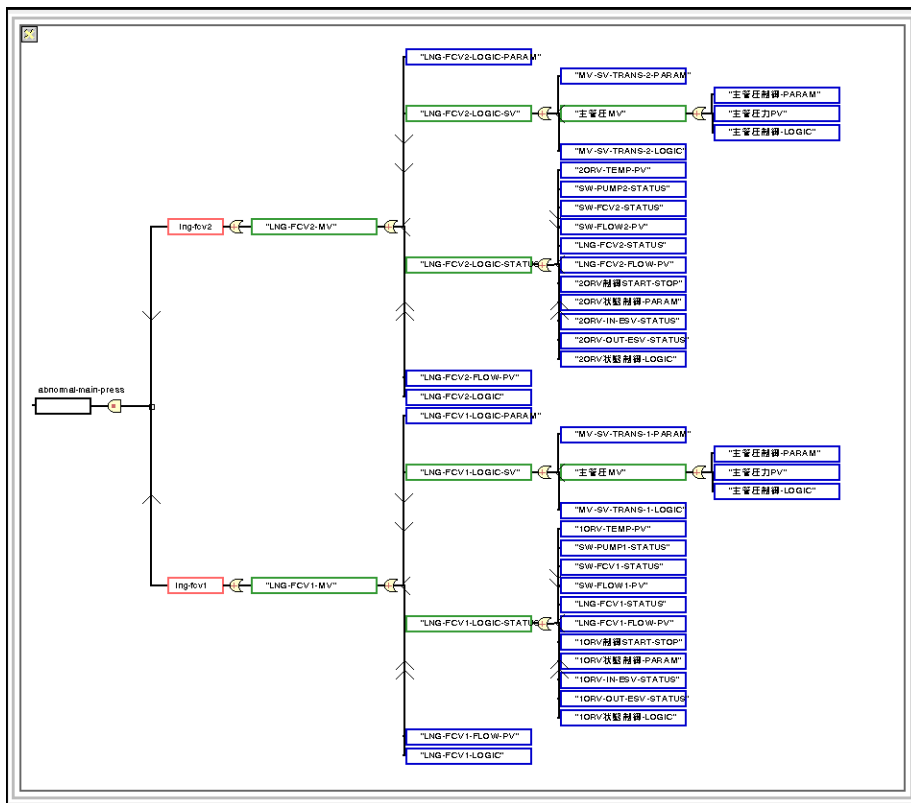


図 4 - 2 - 1 1 トップ事象を出口圧力制御異常として自動生成されたプラント側 FT

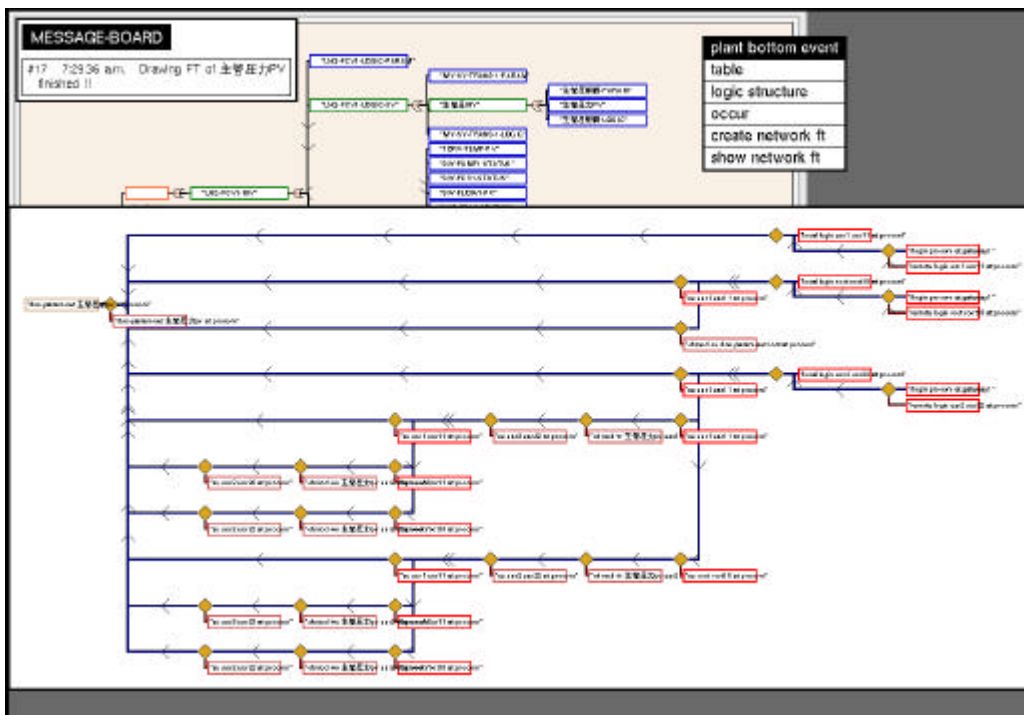


図 4 - 2 - 1 2 制御パラメータ変更に関わるネットワーク側 FT の自動生成

4.2.4 提言、残された課題

セキュリティ・エンジニアリングのフレームワークの検討並びにプラントネットワークに対するリスク分析手法の適用性検討を行った。限られた時間の内ではあるが、FTA/ETA ではプロトタイプシステムの構築まで検討を進めたことで、以下の手法拡張が有効であることがシミュレーションによって示された。

- 1) プラント本体並びに情報ネットワークの統一的表現
 - ・トポロジーの統一構造化表現
 - ・脅威の統一構造化表現
- 2) 動的変化への対応
 - ・構造抽出の自動化
 - ・FT 構造生成の自動化
- 3) 故障・障害波及への対応
 - ・イベント検出とイベント伝播経路探索の自動化

しかしながら、下記のように今後に残された課題も多い。

1) プラント・セキュリティー・エンジニアリング

プラント・エンジニアリングは、基本設計から詳細設計へと各設計の段階に応じた系統的な設計手法とリスク分析手法が既に確立され、プラント・エンジニアリングに対するセーフティ・エンジニアリングの位置づけが確定している。

これに対し、ネットワーク・エンジニアリングは、基本設計、詳細設計の流れの中での系統化されたネットワークの設計手法が今のところ定まっていないように思われる。このことが、セキュリティ・エンジニアリングのためにネットワーク用リスク分析手法を系統化して纏めていく上でネックになる可能性がある。したがって、基本設計・詳細設計の流れの中で系統化されたネットワークの設計手法の検討が必要である。

2) プラントネットワークに対するリスク分析

FTA・ETA, HAZOP を拡張することで、既知の情報に基づいたリスク分析は可能であると考えられる。しかしながら、不正アクセス等に対する十分な対策を採るには、変化の激しいネットワーク構造(関連するハードウェア並びにソフトウェアを含む)を常に追いかける必要がある。これは、ユー

ザのみでは対応できないことであり、少なくともプラントネットワークに関わるハードウェア並びにソフトウェアベンダーは、FTA・ETA、HAZOP等のオープン化されたりリスク分析手法による自社製品の分析結果をユーザに示す必要がある。

また、FTA手法で示したようにネットワーク構造（関連するハードウェア並びにソフトウェアを含む）のモデル化は、不正アクセスを統一的に記述することを可能とする。専門化会議の席上も、このモデル化は日米で協力すべき分野であることが確認されており、協力体制を含めて今後の課題として残されている。

3) その他の課題

上記のほか次のような課題が残されている。

- ・実証試験システムの開発の必要性
- ・リスク回避手段の最適投入に関する指針の策定
- ・セキュリティ・ポリシーに対する人的要因に関するリスク分析
- ・FTA用の確率情報の収集

4.3 セキュリティ評価基準

制御系システム設計時における、そのセキュリティ要件を明らかにする試みとして、近年セキュリティ評価認証の分野で国際的に相互認証を行う動きのあるコモン・クライテリア（ISO/IEC 15408）の枠組みをもとに、その可能性を模索してきた。ネットワーク・システム全体のセキュリティ要件を明らかにする際には個別製品のセキュリティ要件を抽出する場合とは異なり、いくつかの困難を伴う。抽象的な制御系システムを想定し、それが要求する非技術的な管理・運用を仮定した。これによって、これまで記述されることの少なかった制御系システムについて、セキュリティ上の論点を鳥瞰することができると思う。

4.3.1 背景

近年、クリントン政権下の米国においては国家情報インフラストラクチャの保障（アシュアランス）が、国家的な課題として掲げられている。1998年にPDD63（President Decision Directive 63）が指令されて以降、金融、発電、交通等の重要インフラストラクチャ保護の取り組みが開始された。2000年1月には、「情報システム保護のための国家計画 バージョン1.0」が発表され、この中においても政府機関を情報セキュリティのモデルとなるようにすることとともに、重要インフラストラクチャを防衛するために官民の協力関係を築くことが示されている。

重要な国家インフラストラクチャを構成するシステムといえども、その形態、技術的性格は、業種によって様々である。大規模プラント・システムにも、国民生活の基盤にかかわる国家的・社会的な重要性をもつものがあり、石油精製、電力発電、ガス等のプラント・システムの安定的な稼働が求められている。制御するための情報システムには、ネットワーク情報システムが含まれるが、これらは金融情報システムなどとは異なる情報システムである。

制御系の情報システム（以下、制御系システムと呼ぶ）は、国民生活の基盤として、情報セキュリティが強く求められているが、これまでその情報セキュリティの観点から取りまとめられた文献は極めて少ない。また制御系システム自体のあり方も変化しつつある。まず、分散化・ネットワーク化が進むと同時に、独自のプラットフォームで稼働していたシステムが市販のプラットフォームで稼働するようになりつつある。また、制御システムの現場デ

バイスの部分もアナログによる制御が現状は主流であるが、デジタル通信によって制御を行うための検討が進行中である。

ネットワーク接続の進展に関連して情報セキュリティの観点から、このような制御系システムが事務系の情報システム(以下、情報系システムと呼ぶ)との接続や、公衆回線やインターネット経由のリモート監視/リモート・メンテナンスの要請は、どの範囲のネットワーク・システムを守るのかという「セキュリティ境界」の再確認を必要とする。ここにいう「セキュリティ境界」とは、当該情報システムが守るべき情報資産を、その機能的な対策とともに物理的・管理的な対策を併用して守る、セキュリティ・ポリシーが及ぶ範囲を確定する論理的な概念である。

4.3.2 コモン・クライテリア概説と活動概要

制御系ネットワーク・システムについて、典型的なモデルを提示する試みは、当委員会活動の初年度においても、メンバーの共通言語を確立する目的で行われ、中間報告書の中でも示されているところである。2年目以降、制御系システムのセキュリティの機能要件、すなわち当該システムに求められるセキュリティ機能を整理する枠組みを、コモン・クライテリア(Common Criteria 以下 CC と呼ぶ。)に求めた。

我々のワーキング・グループ4が活動を開始した時期、CCが国際的なセキュリティ評価基準の枠組みが提案され、国際標準化されつつあった。(*1) 欧米では、1980年代から1990年代初頭にかけて、主に軍事調達を目的として、既に各国固有のセキュリティ評価基準を確立してきたが、それらを国際的に統一した基準書がCCと呼ばれるものである。CCによって、情報技術に関連した製品のセキュリティの度合いを、様々な視点から系統的に評価できるようになる。このような基準を利用することによって、実在しない抽象的なシステムに求められるセキュリティ機能を整理するという課題・目標に向けて、合意を得ながら手続きを進行させることができた。

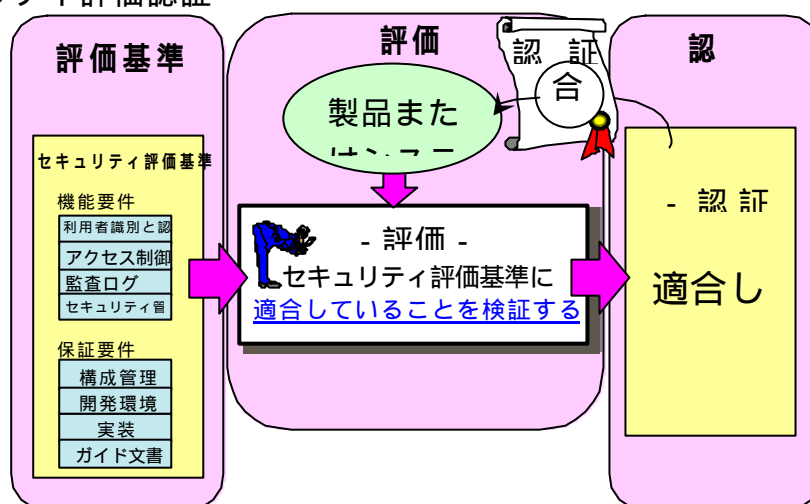
(1) コモン・クライテリア概説

CCが想定しているセキュリティ評価・認証とは、情報システムやそれを構成する機器・ソフトウェア(オペレーティングシステムを含む)について、セキュリティ機能、および、目標とするセキュリティレベルを、評価

基準に基づいて評価し、その結果を公的に検証し、公開することである。評価するのは、政府や民間の第三者機関が行い、これらの機関の評価結果に基づいて、認証機関が評価に合格した製品やシステムに対して認証書を発行し、認証製品リストを一般に公開することになる。

これにより、ユーザ企業は、認証製品を安心して利用することができ、開発企業は、安全性の高い製品やシステムを提供していることを利用者にアピールすることができる、などの効果を得ることができる。

図 1：セキュリティ評価認証



CC は、下記の 3 部から構成されている。

- Part1：一般モデル
- Part2：機能要件
- Part3：保証要件

Part1には、CCが前提とする、セキュリティコンセプトや評価コンセプト等について記載されている。さらに、セキュリティ評価の基本となる、評価対象製品やシステムのセキュリティ仕様書である「セキュリティターゲット」(Security Target、STと略称)や、STのベースとなる文書である「プロテクション・プロファイル」(Protection Profile、PPと略称)について解説されている。

Part2には、製品やシステムが備えるべきセキュリティ機能(監査、暗号、

ユーザデータ保護等)に関する要件(「機能要件」と呼ばれる)が規定されている。この機能要件の整理が重要な作業であると認識され、注力された。

Part3には、Part2の機能要件を確実に実装にブレークダウンするための要件(開発仕様書の内容、テスト実施内容、脆弱性/誤使用に対する抵抗力、構成管理、開発環境、配布手順等、「保証要件」と呼ばれる内容)が規定されている。また、開発者が評価者に提出すべきドキュメント類や、評価者が実施する評価内容が、抽象的ではあるが規定されている。さらに、製品やシステムが機能要件をどこまで保証しているかを表す尺度として、各保証要件のサブセットという形で7階層の「保証レベル」(EAL: Evaluation Assurance Level と呼ばれている)が定義されている。

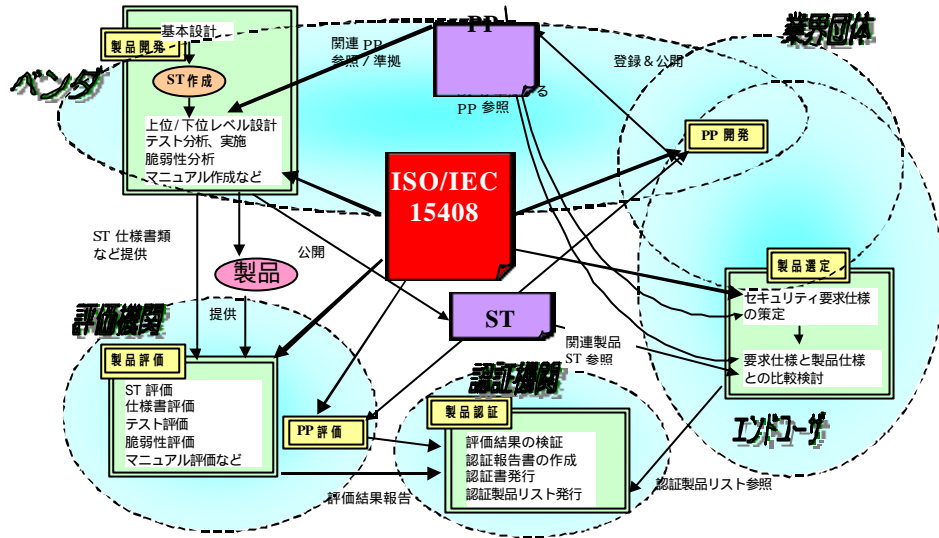
この枠組みにおいて、実際に評価基準に相当する部分はPPである。この枠組みは、相当の客観性と普遍性が期待できると考えられたので、これに基づいて、制御系システムに要求するセキュリティ要件を PP として記述することができないかが検討された。

情報技術セキュリティに関連する製品やシステムの開発にあたり、そのセキュリティ仕様を明確にすることが必要になる。開発者は、その製品やシステムが想定する利用条件や脅威、脅威に対する対抗方針、対抗方針を実現するために必要な機能要件、製品の具体的なセキュリティ基本仕様、EALなどを記述したSTを作成する。製品やシステムの評価を受ける際、開発者はSTを評価者に提供する。STはセキュリティ評価の出発点になる。

製品やシステムのSTは、開発者の意向により、ユーザに公開することができる。ユーザはSTを参照して、その製品やシステムが前提とする脅威やそれに対抗したセキュリティ機能、およびその機能がどこまで保証されているのかを知ることができる。

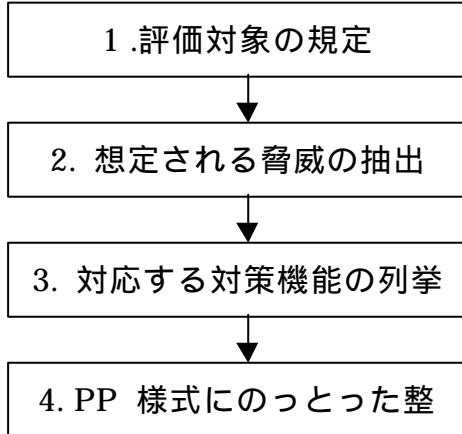
一方、製品やシステムの種別ごとに、考慮すべき脅威やその対策、対策を実現するためのセキュリティ機能要件や保証レベルなどの事項を記述した文書がPPである。PPにもSTと同様な項目が記述されるが、STと異なり、具体的な製品やシステムのセキュリティ基本仕様は含まれない。

図 2 : ISO/IEC 15408 (Common Criteria)



PP の策定にあたっては概ね 図 3 に示される作業が必要となる。

図 3 : プロテクション・プロファイル (PP) の作成手続き

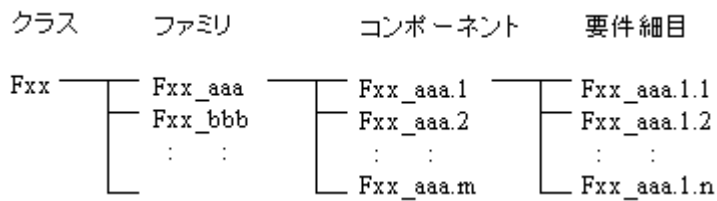


(2) 活動概要

概ね PP を作成手続きに従って活動したが、PP 様式の学習そのものが主たる課題ではないので、セキュリティ機能要件を整理する試みにとどまった。

図3において、「3. 対応する対策機能の列挙」において列挙される対策機能は、「4. PP 様式にのっとりた整理」において階層化・整理された基準書である CC の中から適当な要素を抽出することによって、整理される必要がある。図4は、機能要件の階層構造を示すものである。

図4：機能要件の階層構造



機能クラスには、図 5 に示す 11 のクラスがある。

図 5：機能クラス

機能クラス	略称	概要
監査 Security audit	FAU	セキュリティ事象に関連した情報の認識、記録、保存分析に関する要件
通信 Communication	FCO	データ通信への参加者の識別を保証する否認防止に関する要件
暗号サポート Cryptographic support	FCS	暗号鍵生成 / 配布 / 失効の管理、データの暗号化 / 復号、デジタル署名の生成 / 検証等の暗号操作に関する要件
ユーザデータ保護 User data protection	FDP	アクセス制御、情報フロー制御、ユーザデータのインポート / エクスポート時のセキュリティ属性保護、ユーザデータ転送時の機密保護等に関する要件
識別と認証 Identification and authentication	FIA	ユーザのアイデンティティを確立し検証する要件
セキュリティ管理 Security Management	FMT	セキュリティ属性や、セキュリティ機能に関連するデータ (ex. 認証データ、セキュリティ方針 DB) 等の管理に関する要件
プライバシー Privacy	FPR	他者によるアイデンティティの発見 (探り出し) と誤使用の防止に関する要件
TOE セキュリティ機能保護 Protection of the TOE Security Function	FPT	セキュリティ機能を提供するメカニズムと内部データの正当性および保護に関する要件
資源利用 Resource utilization	FRU	資源の耐障害性、優先度制御、資源割り当てに関する要件
TOE アクセス TOE access	FTA	ユーザセッション (TOE と利用者との間の対話路) の制御に関する要件
信頼経路 / チャンネル Trusted path/channels	FTP	利用者と TOE との間の高信頼性通信路に関する要件

これらのルールに精通することが主たる目的ではないので、3. 対応する対策機能の列挙までの活動に注力した。

*1 ISO/IEC/JTC 1/SC 27/WG 3 から Common Criteria v.2 が提案されて、国際標準 (International Standard 15408) となった。

4.3.3 想定するモデル (TOE)

セキュリティ機能要件を整理することを試みた対象は、制御系システムである。これについて抽象的な概念モデルを設定し、典型的な機能要件を抽出することを試みた。

我々が本作業を開始した時点において、存在していたPPは、いずれも個別製品分野についての評価基準であり、ネットワーク・システムのPPとして参考になるものは、見あたらなかった。例えば、リレーショナル・データベース製品や、パケットフィルタリング・ファイアウォール製品についてのPPなどは存在していたが、複数の製品を組み合わせて構築されるネットワーク・システム全体についてのPPは存在していなかった。PPが求めているものは様式であり、その中で評価対象が規定され、想定される脅威が列挙されて、それらに対応する対策機能が示されることが本質的な作業である。PPは、いわば、その作業によって抽出された項目を記述する雛形であるといえる。対象が明確に規定することができれば、必ずしも個別製品である必要はないと考えられた。

一方で、個別のコンポーネントのセキュリティ要件が規定され、それを満たすコンポーネントで構成されたネットワーク・システムならば、全体としてのセキュリティも確保されるのではないかと、という考えをもたれることもある。残念ながら、たとえ個別製品がセキュリティ機能要件を満たしているとしても、それらで構成されるネットワーク・システムが高いセキュリティ機能を持っているとはいえない。たとえば、ネットワーク環境にはネットワーク環境固有の脅威があり、それらについての対策機能が求められる。

制御系システムのネットワークを対象とするPPの作成を試みが、ネットワーク・システムを対象とすること自体が一つの試みとなった。ネットワーク・システムを対象とする際には、そのネットワークの範囲を示す必要がある。背景でも述べた通り、ネットワーク接続は、ますます進展しつつあり、対象ネットワークを切り出したモデルとして規定する必要がある。

「制御系」を対象としたのは、「脅威」の範囲が広い、すなわち通常の事務系の情報システムにはない固有の「脅威」が存在するからである。例えば、まさに物理量の制御を行う装置（デバイス）とそれを制御する機器（コントローラ）の周辺、さらにそれらを統合管理するコンソールは、制御系システ

ム固有の機器・装置であり、相互に密接な関係がある。これらについて想定される脅威と、対策機能が明確に示されるように、通常の事務系の情報システムを含まない部分として対象を規定した。

個別装置やシステムの一部ではなく、その「ネットワーク」を対象としたのは、それらが相互に密接な関係をもっていることとともに、最初の1歩として制御系システムに存在する「脅威」と「対策機能」の鳥瞰を得ることができると考えられたからである。この中で今後、個別装置に求められるセキュリティ機能を検討していく際に、全体的な枠組みの中に位置づけて検討することができるようになると考えた。

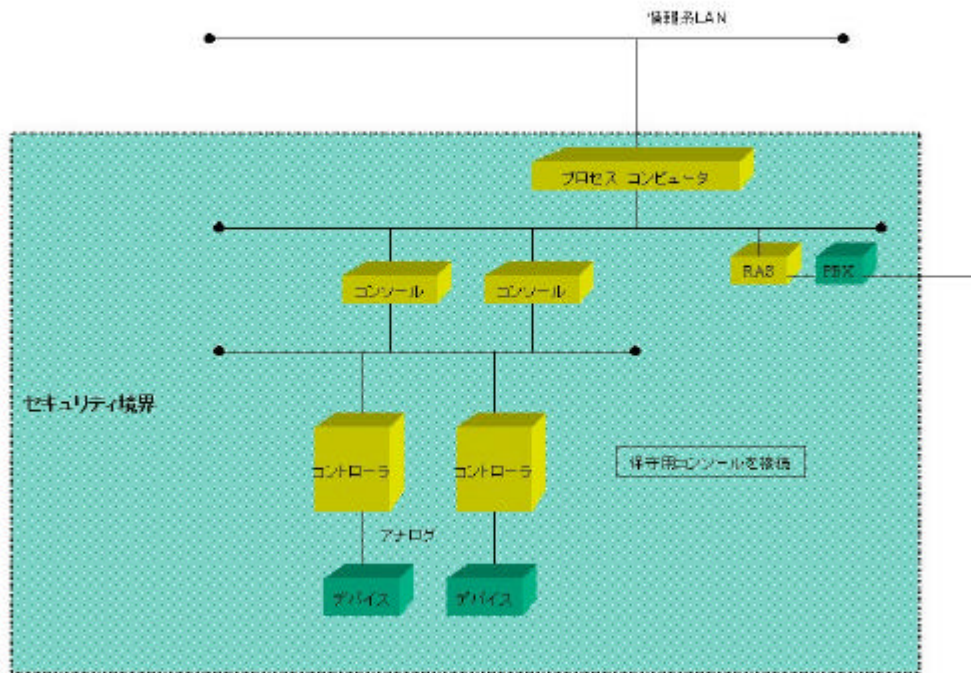
TOE を想定する際に、このような「セキュリティ境界」としての範囲の限定を行うとともに、そのTOEが利用される上での前提事項を仮定する必要がある。後述するように、ネットワーク・システムを対象とするにあたって、その管理・運用の仮定を設けることが必要となり、それは個別製品に対して設ける仮定よりもタイトなものとなったように感じられる。

次頁に、図 6： TOE (Target Of Evaluation) を示す。

情報系システムからは分離された、制御系システムを想定する TOE とした。制御系システム内には、複数のコンソールが制御系情報 LAN にあり、制御 LAN も複数あるシステムを想定する。また近年、上述のネットワーク構成は、アナログのデバイスが前提となっていることから、標準化が進められつつあるフィールドバスは想定せず、アナログのデバイスとコントローラを前提とする。

これらすべてについて、システムのセキュリティ機能では対応できない脅威については必要なすべての物理的・管理的な対策がとられるものとする必要がある。ここで、コンソール等の機器に対する物理的なアクセスは、適切な入退出管理によって認証されていない人間が操作する脅威を防ぐという仮定を設ける。さらに、コンソール等の機器の操作権限について、その組織体の意思を反映するセキュリティ・ポリシーにのっとり、それぞれの操作の権限者が定められていることを仮定する。

図 6 : TOE (Target Of Evaluation)



4.3.4 脅威と対策機能の洗い出し

中間報告書においても、数々の「脅威」が認識されていた。しかし、対象とすべきモデルも、その編集の最終段階でようやく、共通認識ができるもののイメージが描けたにとどまった。前述のTOEについて、想定される「脅威」と対応する「機能」を対で洗い出すためのブレン・ストーミングを繰り返し、時にはベンダー企業を見学し、エンジニアとのディスカッションをかさねた。このようにして得られた「脅威」と「機能」を下表のように整理した。また、CC の第1版にあった（現行第2版、すなわちISO/IEC 15408にはない）、Annex B (*2)の脅威項目にも、参考とすべく目を通した。残念ながら、この資料からは项目的には得るものは少なかったが、PP作成作業を一通り追体験することができた。

	脅威	対策機能
<p>プロセス・コンピュータ</p> <p># 前提 情報系 LAN 側からのコンソールやコントローラ上の情報の要請は高まりつつある。 情報系 LAN も、次のコンソールのレイヤー（制御系情報 LAN）も汎用的なイーサネットや TCP/IP のプロトコルが使用されることが多い。ネットワークに接続されるコンピュータのプラットフォームも、市販のオペレーティング・システムが採用されつつある。# また、分散オブジェクトの形態（例：DCOM）で、パラメータなどのデータが、ネットワーク上を転送される機能が動作しうる。</p>	<p>情報系 LAN 側のユーザが何らかの手段でコンソールのレイヤー（制御系情報 LAN）上のアカウントの認証を得た場合、 本来、権限外の情報系 LAN 側のユーザが、コンソールを操作する可能性がある。</p> <p>コンソール上のデータやソフトウェアが、コンソール側の方針に反して改ざんされる可能性がある。</p> <p>+ 利用可能性を妨げられる可能性がある。</p>	<p>情報系 LAN 側のユーザを認証する機能。</p> <p>情報系 LAN のユーザが要請するコンソールやコントローラ上の情報を複製・保有する機能。</p> <p>制御系情報 LAN への直接的な接続を禁止する機能。</p> <p>アクセスを記録し保持する機能。</p>
<p>制御系情報 LAN について</p> <p># 前提 #このレイヤーには、汎用的</p>	<p>1. 権限を越えたコンソールの操作ならびに権限外のコンソールの操作の脅威（オペレータの権限を上回る操作や外部の侵入者による操作</p>	<p>1. システムにアクセスするすべての個人を、個人単位で認証し、その属性に基づいて、資源へのアクセスを制御する機能が必要である。</p>

<p>なイーサネットや TCP/IP のプロトコルが使用されることが多い。ネットワークに接続されるコンピュータのプラットフォームも、市販のオペレーティング・システムが採用されつつある。</p>	<p>の脅威)についてオペレータにも技能的な習熟の程度や、経営管理機構上の要請に基づきアクセス可能な資源をコントロール可能としなければ、未熟な操作や、経営管理機構上の要請に反する操作ができてしまう。同一のレイヤーのネットワーク(制御系情報 LAN)上には、エンジニア用のコンソールも配置される。エンジニアの経営管理機構上の権限を超過した操作が行なわれる可能性がある。</p> <p>2. リモート アクセスについて</p> <p># コンソールをユーザの要請に基づいてこのレイヤー(制御系情報 LAN)上に、ベンダーがリモートからアクセスして監視する要求もある。これは、あくまでも、ユーザの要請(エラーメッセージの意味の解析等)に基づく監視である。</p> <p>リモートから電話回線経由のアクセスにおいて、ソフトウェアプログラムをベンダーがアップデートする等、リモート メンテナンスの要請もある。</p> <p>もし、この作業を行うリモートのベンダーの認証に失敗した場合には、不適切なソフトウェアが、当該レイヤーにあるコンソールホストに搭載される可能性がある。</p> <p>3. オペレータの管理可能性について</p>	<p>情報系 LAN とは独立したアカウント管理機構とし、情報系 LAN のアカウントを受け入れる信頼機能をもってはならない。</p> <p>このアカウント管理機構自体を操作する権限は、経営管理機構の意思を代表する個人が特権としてもつことができる機能体系。</p> <p># このようなアカウント管理の機構が、各工場の制御系情報 LAN ごとに必要。</p> <p>2. # リモートから、ベンダーに監視(エラーメッセージの意味の解析等)を依頼する場合などにおいてリモートアクセスのセッションをはるのは経営管理組織の意思に基づくユーザの側からの接続のみ可能とし、外部からの一方的な接続を拒否する機能。</p> <p>3. 監視義務の限度設定機能。方針に基づく、警告の設定機能。</p>
--	---	--

	<p>また、オペレータにも人間として、監視能力の限界があるので、過大な監視義務を負うことは、警告の見落としにつながる可能性がある。一方、頻繁な警告は、オペレータの重要性の判断を誤らせる可能性がある。</p> <p>4. 監視可能性の確保について</p> <p># コンソールが1機しかなく、何らかの事情で、そのコンソールでの監視が行えない場合、全く監視できなくなってしまう。</p> <p>5. 操作の記録の確保について</p> <p>例えば、コンソールに対するネットワーク経由の操作が記録されない場合、たとえ直接のコンソールの操作が記録されていても、不正な操作を事後的に検知することができない。</p>	<p>4. # 常時、監視可能性を確保するため、コンソールは複数台、接続されている必要がある。</p> <p>5. パラメータ設定データ、ソフトウェア プログラムの更新を含む、各種オペレーションや警告について、後日、検証可能なログを生成する機能。</p> <p>ネットワーク経由の操作を含む、すべての操作を記録できるようにする機能。これらの操作記録が改ざんされないよう、安全に記録を保持できるようにする機能。</p>
<p>「制御系情報LAN」と「制御LAN」の接続について</p> <p># 前提 コントローラは、「制御系情報LAN」上に設けられるのオペレータのアカウントが管理する対象となる。コントローラが扱うパラメータを分散オブジェクト（例：DCOM）の形態で保持し、上位のレイヤー（コンソールのレイヤー以上）とのデータ交換、すなわちチューニングなどをおこなう動きがある。このような分散オブジェクトには、原料の配合比率や操業度などの企業秘密が含まれる可能性がある。</p>	<p>コントローラのパラメータが、不正に読み出し・更新される可能性がある。</p> <p># 分散オブジェクトの形態でのパラメータの不正な読み出し・更新も含まれる。</p>	<p>パラメータの読み出し・更新を行える者をコントロールする機能。</p> <p># コンソール上のオペレータのアカウントが管理する。</p>

<p>コントローラ自体について</p> <p># 前提 今回のアナログ デバイスのコントローラを前提とする。コントローラには高いアベイラビリティ（可用性）が要求される。コントローラのメンテナンスの必要から、コンソール レイヤー（制御系情報 LAN）からの通信が機能しない事態において、コンソール レイヤー（制御系情報 LAN）以外の端末を接続する要請はある。</p>	<p>1. コントローラが何らかの理由で動作しなかった場合、デバイスの意図された動作が保証されない。</p> <p>2. コントローラが、予定されたコンソール レイヤーのエンジニアリング端末等以外とネットワーク接続できる場合、不正に操作される可能性がある。</p>	<p>1. 高いアベイラビリティ（可用性）</p> <p># これを確保するため、冗長化された CPU・プロセッサを動作させることが必要である。</p> <p>2. # コントローラ自体のメンテナンスのために臨時に接続する端末が、ネットワークを利用する機能（センサーやバルブ等のデバイス、コンソールとの通信機能）の禁止が必要。</p>
<p>コントローラとの接続について</p> <p># 前提 フィールドバス規格に基づいて、デジタルによる情報伝達が拡充される動きがあるが今回の PP ではアナログを前提とする。 現状では、各種パラメータをアナログ データ（電圧の強弱）としてコントローラとの間の通信に利用しているのが基本形態である。ベンダー各社は、独自に追加的な情報伝達機能を追加拡張している。センサーやバルブ等のデバイスが本物であるか、をコントローラ側で検証する機構はないのが実状である。</p>	<p>アナログ デバイス（センサー、バルブ等）の不正な物理的取り替えを検知できない場合、意図とは反する動作をする可能性がある。</p>	<p>アナログ デバイス（センサー、バルブ等）の不正な物理的取り替え、非連続的な変化を検知する機能。</p>

注)

で記述される前提事項は、読者の理解の便宜のための事項であり、PP に記述されるものではない。

4.3.5 プロテクション・プロファイル (PP)

PP の記述を実際に英語で行うことを試みた。適当な機能クラスの要素を見つけれない項目もあり困難な作業であった。また、後述するように、これが読者にとって読みやすい形態、項目の並びであるか、疑問である。

4.3.6 成果

セキュリティに関して固有の「脅威」をもつ「制御系システム」について、自らのセキュリティ機能と物理的対策・運用管理的対策によって保護されるべきネットワークの「セキュリティ境界」とするモデルを提示した。そして概念モデルとして「制御系システム」を構成する主要な各機器がもつ「脅威」と「対策機能」の鳥瞰を得ることができた。

4.3.7 課題

(1) システムを対象とする PP を記述することに内在する課題

一般に、あるシステム、およびそれに含まれる情報のセキュリティを確保する場合に、技術的な対策と、その管理・運用は補完的関係にあるといわれる。技術的な対策機能が明確になると、それに対して補完的な関係にある管理・運用が明確になる関係が存在する。しかし、システムの PP の記述においては、事前的に TOE が使用される上での前提となる管理・運用が仮定されねばならない。事前に、普遍性のある管理・運用を仮定することは困難である。ひとつの仮定として受容するしかないであろう。

この仮定において、経営管理上の権限範囲を想定するので、経営管理のあり方に対して要求する内容を含んでいる。(つまり、「制御系システム」がその管理者権限を規定することになる。)例えば、情報系システムの管理者との権限の配分、全社的に共通管理されていることが多い情報資産の扱い (PBX 構内回線の扱い等) などについて、その管理体制について要求することになる。システムの機能が、経営管理上の権限・機構を規定する逆の論法になっているとも受け取られうる。この妥当性については、別途、検討する必要があるだろう。

(2) PP 記述形式上の課題

図3の「4. PP 様式にのっとった整理」において、製品の PP と同様にすべての部分、コンポーネントにおける脅威と対策技術をアルファベット順に並び替えると、それらが入り乱れ、それぞれの位置づけがわかりにくくなってしまふ。ドキュメント作成過程において、その修正・更新も容易ではない。

(3) 個別機器の PP 検討への発展可能性

TOE の確定作業において、我々は制御系システム部分の全体を対象とした。この中で、各機器、コンポーネントの位置づけ、そのセキュリティ機能要件が明確になってきたものとして、以下に例示する。

プロセス・コンピュータの位置づけ

「情報系システム」側からの情報要求に応える機能を持つ装置として位置づけることができる。同時に「情報系システム」側からのセキュリティ侵害の経路となりうる装置ともいえる。「制御系システム」全体を境界において守るのに必要なセキュリティ機能が実装される装置として期待される。

コンソール

経営管理組織の該当部門の権限管理機構をシステムの的に反映しうる権限管理機能の必要性が求められる。権限管理の対象となるシステム上の資源は「コントローラ」に限らず、今回のセキュリティ境界内にある「プロセス・コンピュータ」や「RAS」も対象となるはずである。

このような位置づけを前提に、個別の PP を策定していくのは有意義であると考えられる。

第5章 今後の課題

第3章、第4章の各項において、また、資料編の「WG活動報告」において、今後の課題を記述しているが、ここでは、3年間の委員会活動の終了に際して、全体的な視点から今後の課題に述べる。

大規模プラントに対象を絞って関連諸問題の調査、研究を行ったが、問題の本質および委員会活動に関する時間的制約から、その成果は完璧なものにはなっていない。しかし、そのような成果であっても、関心を持つ方々にそれらの理解を求め、個別の問題として発展させていただくことが求められる。

デジタル・ネットワーク社会に突入し始めた今日、情報セキュリティ問題は新たな社会問題であるから、課題は際限なく列挙されるが、そのうちから優先的に取り上げられるべきと考えられる幾つかのものを記す。

* セキュリティに対する理解を啓発する活動

「第3章 非技術系事項の報告」の「3.1 セキュリティ・マネジメント」において述べたとおり、社会全般の情報セキュリティに対する意識改革が最も肝要である。

啓発活動では、対象者を特定化する工夫（たとえば、企業経営者、技術者など重層的に特化する）が必要である。また、平成11年の情報化月間に開催したシンポジウムと同様の機会を継続して設けるなど社会的課題としての位置付けることも重要である。

* セキュリティ問題を継続的に取り扱う機関の設置

本委員会は期間限定で活動してきたが、今後の技術進歩や海外の動向などについて継続的に関心を持ち、調査、公表などを行うことが必要である。

特に、継続的な国際交流は不可欠であり、ボーダレスな環境を考えると我が国の関係者の交流がなければ、セキュリティについての十分な対応が不可能である。専門家育成や対策研究などの役割を含めて、専門機関を常設することが必要である。

* 実証的な横展開の活動

本委員会はプラント・ネットワークを対象として調査研究したが、その成果を個別のプラント・ネットワークに当てはめて行う実証的な事例研究が必要である。問題の性質上、個別の研究内容の大部分は非公開となるが、本委員会の成果に対する評価部分が公開されれば有用である。

また、本委員会と同様の活動が、他産業においても展開されることが必要である。

* その他の課題

プラント・ネットワークのセキュリティ分析手法などの技術開発に関する研究課題、セキュリティ評価の定量化などの理論面の研究課題、およびプラントの運用におけるセキュリティレベルの向上、必要な改善策についての研究課題など多数残されている。詳細はWG活動報告を参照していただきたい。

あとがき

今日の経済社会のデジタル化の奔流は、世界的なニュー・エコノミーあるいは産業革命以来の新しい経済社会革命の序章といわれるほど、日々、力強く、グローバルな広がりをもって加速しております。我が国の電子商取引の市場規模は、私どもの予測では、2003年には、昨年約8倍にも拡大し、約72兆円に成長すると見込んでおります。他方、このようなデジタル化は、新たな脆弱性を伴いつつ発展していることも事実であります。

折しも昨年来のコンピュータY2K問題がこれを浮き彫りにいたしましたし、ハッキング、クラッキング、不正アクセス、サイバーテロ、インフォ・ウォーといった従来一般には耳慣れなかった言葉が、今日では新聞紙面ににぎわしている状況にあります。

大規模プラント・ネットワーク・セキュリティ対策委員会は、石油精製、石油化学、電力等、経済社会を支える重要なインフラストラクチャーである大規模なプラントの制御系システムを対象に、標準プロトコルを用いたオープンシステム間の相互接続へと発展してきている状況をいち早く捉え、平成9年9月にその脅威からの防御策の検討に着手し、さらには、サイバーテロに関する我が国で初めてともいえる本格的検討の場として注目を集めてまいりました。平成10年3月にまとめていただいた中間報告に示された問題提起と対策の方向性は、世間の大きな注目を浴びたところであります。

そして、今般、おまとめいただいた最終報告は、アンケート等を通じた実態把握、国際的な調査等を行いつつ、技術的事項・非技術的事項を総合的に論じた画期的なものであり、今日、ようやく官民の関心が高まりつつあるネットワーク時代の重要インフラの防御の在り方に共通する課題と対策を示していただいたと理解しております。

3年にわたる検討の過程において、情報セキュリティの重要性に関する認識は、ネットワーク化の進展とともにますます高まりました。本年2月13日には、通商産業省等を主管とする「不正アクセス行為の禁止等に関する法律」が一部を除き施行されております。また、昨年9月に内閣官房に設置された「情報セキュリティ関係省庁局長等会議」においては、高度情報通信社会を迎えるに当たっての法制度の問題、ハッカー対策、更には、重要インフラに対するサイバーテロ対策を政府としてとりまとめることとされ、本年1月にまず「ハッカー対策等の基盤整備に係る行動計画」が決定されました。

一方、その直後に発生した政府機関等のホームページ改ざん事案等にかん

がみ、政府は、本年3月、内閣官房に「情報セキュリティ対策推進室」を設置するとともに、内閣総理大臣を本部長とする高度情報通信社会推進本部に「情報セキュリティ関係省庁局長等会議」を発展的に改組し全省庁を構成員とする「情報セキュリティ対策推進会議」の設置及び民間の有識者からなる「情報セキュリティ部会」を設置するなど、官民連携の下、政府全体としての情報セキュリティの取り組み体制を抜本的に強化いたしました。そしてこれらの政策立案の過程で、先駆的な本委員会での検討内容が幾たびか紹介され、直接的・間接的に貢献してまいりました。

ネットワークは日々発展しており、今日、ネットワーク・セキュリティは、情報通信社会の構築のために重要かつ不可欠の事柄として認識されています。このような意識の高まりは大変好ましいものでありますが、他方で「コンピュータ・ネットワークは危ない」といった漠然とした不安から情報化に後ろ向きな姿勢をとるのではなく、冷静に脅威を分析し具体的な防御対策を講じつつネットワークを有効に活用しようという前向きな考えを持つことがますます重要となっていると考えます。

ネットワーク・セキュリティは、防御側の対策が最も重要であり、かつ、基本であります。自由な参加によって発展してきたネットワーク社会の特長を十二分に生かしていくためにも、企業経営者をはじめとするネットワーク利用者自らが、リスク・マネジメントの観点からの効率的かつ総合的な防御対策を技術・組織・人を有機的に組み合わせることにより講じていくことが求められます。

本最終報告書は、これまでの委員会での活動を集大成したものでありますが、基本的な方針として、本委員会が、常に実証的かつ実践的な立場から検討を重ねてきたという点は特筆されるべきであり、官民が一体となった取り組みの重要性と有効性を示しているものと考えます。特に、官民による取組の重要性は、本年1月クリントン大統領が発表した米国の新しい重要インフラ防護政策の中核をなすものであり、我が国政府としても、先に述べたが如く、新しい官民の連携関係を構築しつつあります。

他方、これにより施策の全てが完結したわけでないことは言うまでもありません。制御系ネットワークのセキュリティ技術開発は、更に、具体的な取組みを通じた深化を図る必要がありますし、非技術的事項については、ISO等において国際規格化が進む中で、世界の流れを組み込み、あるいは、これに反映させながら私どもとして検討を続ける必要があります。

また、この委員会での成果を各種の重要インフラの防護に具体的に役立て

ていくことも極めて重要であります。これらは、私どもが預かる課題であると考えており、今後、一層、取組を強化していく所存であります。

最後に、3年間にわたる本委員会における検討を終始リードし、とりまとめまで導いていただいた梅田委員長、関連ワーキング・グループを中心に精力的な活動を続けていただいた各方面の委員の皆様及び事務局を努められた社団法人情報システム・ユーザー協会の皆様に心より感謝申し上げます。

平成12年3月

通商産業省機械情報産業局長
太田信一郎