CSMS 認証制度について

一般財団法人 日本情報経済社会推進協会
情報マネジメント推進センター
副センター長
高取 敏夫

CSMS認証制度について

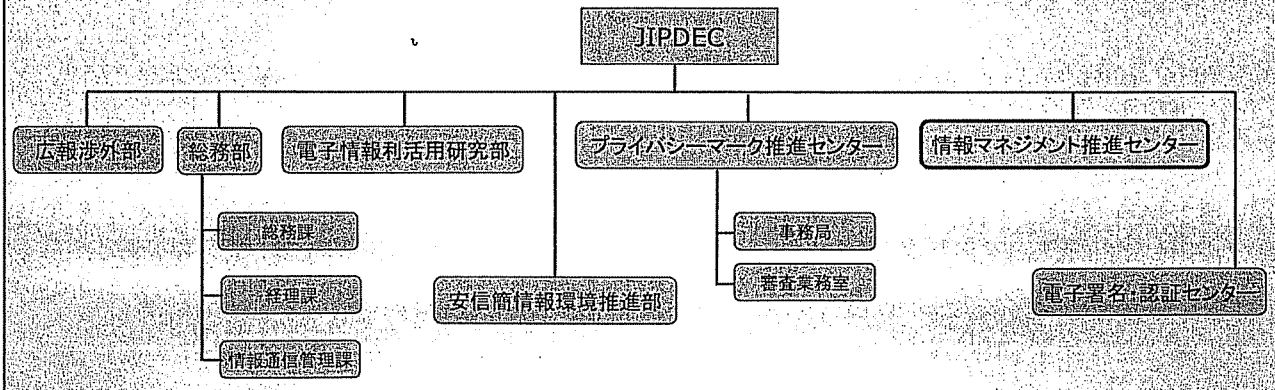
JIPDEC（一般財団法人日本情報経済社会推進協会）
情報マネジメント推進センター
副センター長　高取　敏夫

2014年2月5日

http://www.isms.jipdec.or.jp

JIPDEC組織図

- JIPDEC（一般財団法人日本情報経済社会推進協会）
- 設　立：昭和42年12月20日
- 事業規模：26億4,300万円（平成25年度予算）
- 職　員 数：126名（平成25年4月現在）



情報マネジメント推進センターの主な業務内容

□情報技術に関連するマネジメントシステムの認定機関としての業務及び各制度に関連する普及業務

- ISMS/ITSMS/BCMS認定システム実施に伴う諸業務
- ISMS/ITSMS/BCMS認定審査の実施
- ISMS/ITSMS/BCMS関連の委員会事務局業務
- IT資産管理(ITAM)に関する調査研究業務
- 国際認定機関やフォーラム(IAF、PAC等)との相互連携の推進
- ISO/IECなど(国際規格、ガイド策定等)への積極的貢献
- 制御システムセキュリティ認証基盤整備事業の実施

制御システムのセキュリティを実現するための基準

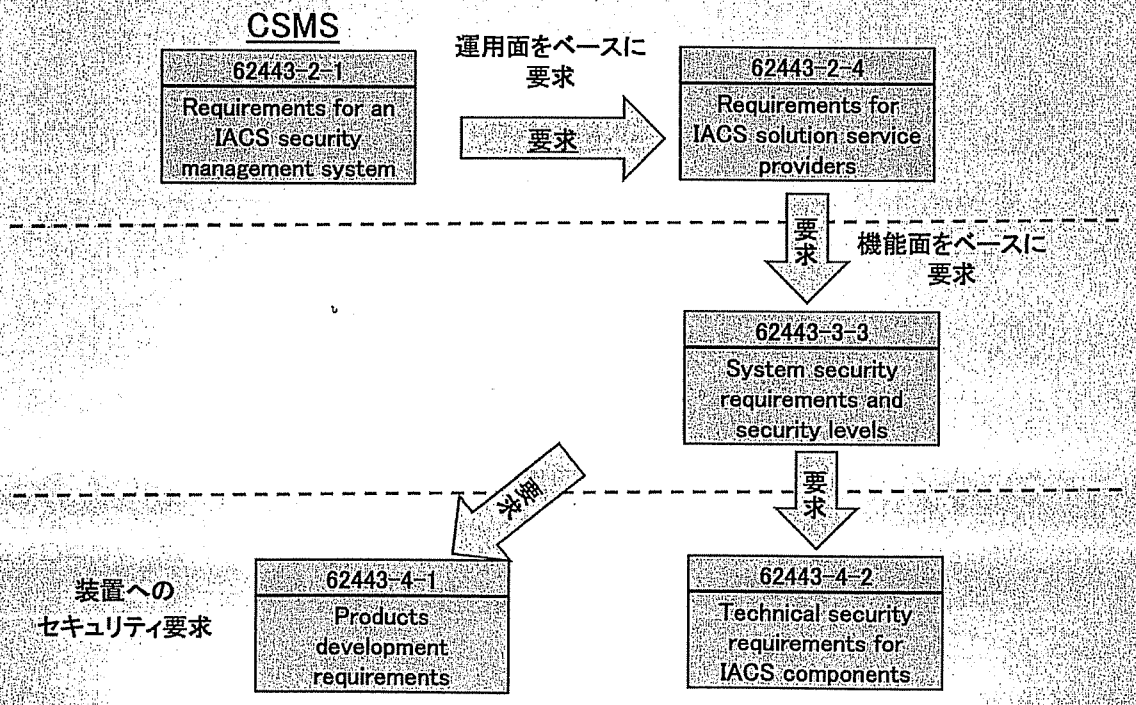
制御システム分野で広く共通的な活用ができる規格であり、制御システムの利用者、装置製造者のそれぞれで広く活用できる規格としてIEC 62443シリーズがある。

- IEC 62443-1 シリーズ ： この規格全体の用語・概念等の定義
- IEC 62443-2 シリーズ ： 組織に対するセキュリティマネジメントシステム
- IEC 62443-3 シリーズ ： システムのセキュリティ要件や技術概説
- IEC 62443-4 シリーズ ： 部品(装置デバイス)層におけるセキュリティ機能や開発プロセス要件

IEC 62443シリーズの対象者

対象者	IEC	原本名
全体	62443-1-1	Terminology, concepts and models (Ed.2)
	62443-1-2	Master glossary of terms and abbreviations
	62443-1-3	System security compliance metrics
	62443-1-4	IACS security lifecycle and use-case
事業者	62443-2-1	Requirements for an IACS security management system (Ed.2)
	62443-2-2	Implementation guidance for an IACS security management system
	62443-2-3	Patch management in the IACS environment
	62443-2-4	Requirements for IACS solution service providers
ｲﾝﾃｸﾞﾚｰﾀ	62443-3-1	Security technologies for IACS
	62443-3-2	Security levels for zones and conduits
	62443-3-3	System security requirements and security levels
装置ﾍﾞﾝﾀﾞｰ	62443-4-1	Products development requirements
	62443-4-2	Technical security requirements for IACS components

IEC 62443シリーズの要求事項



制御システムの サイバーセキュリティマネジメントシステム (CSMS)

- IEC 62443-2-1:2010(Industrial Communication networks – Network and system security – Part2-1:Establishing an industrial automation and control system security program)は、IACS(Industrial Automation and Control System)をサイバー攻撃から保護するための要素を規定している。

[IEC 62443-2-1(Ed.2) Requirements for an IACS Security management system]

- 主要なカテゴリーは、リスク分析、CSMSによるリスクへの対処、並びにCSMSの監視及び改善の3つで構成されている。

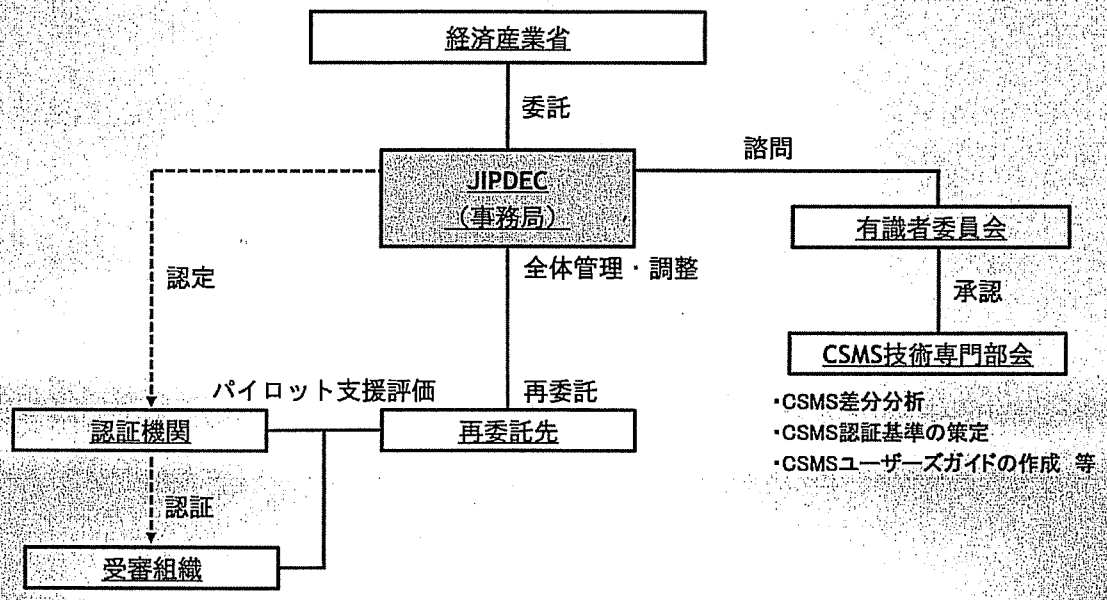
- リスク分析をベースとしたセキュリティマネジメントシステムの構築が可能である。

制御システムセキュリティ 認証基盤整備事業(目的)

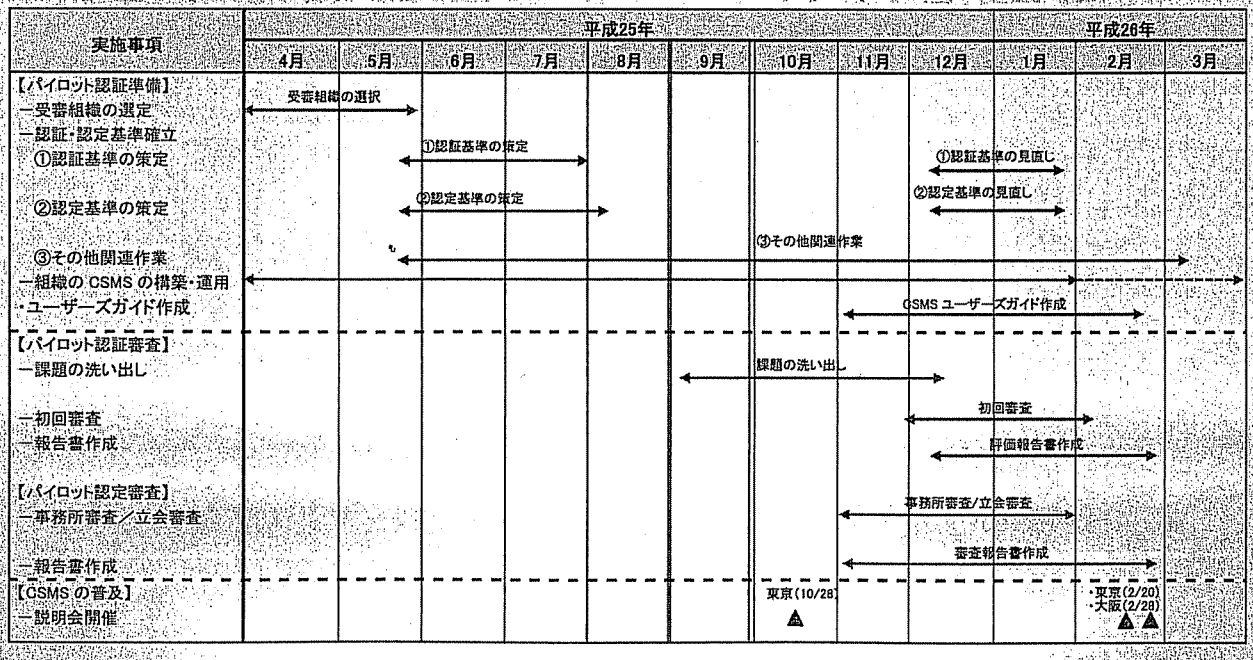
本事業は、制御システムの構築・提供を行う組織や制御システムを運用する組織が、サイバーセキュリティマネジメントシステム(CSMS:Cyber Security Management System)を確立することにより、制御システム分野におけるセキュリティ強化を図ることを目的としている。

- パイロット認証の実施によるCSMS認証基準・認定基準の評価
- CSMS認証基準を用いた第三者認証制度の確立
- 制御システム事業者への普及啓発を目的としたCSMSユーザーズガイドの作成
- CSMS認証の国際的な整合性の確保

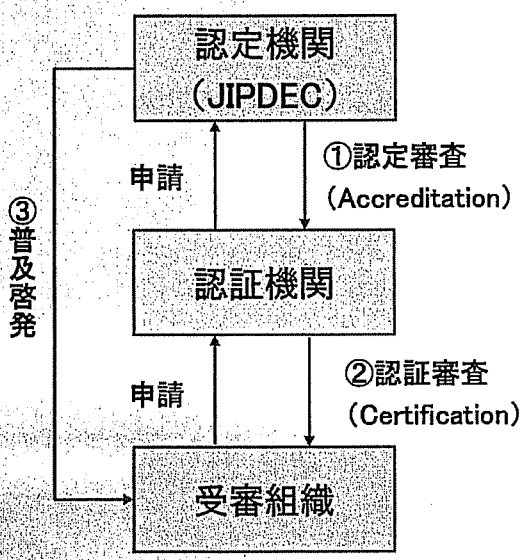
制御システムセキュリティ認証基盤整備事業（実施体制）



制御システムセキュリティ認証基盤整備事業（スケジュール）



CSMS認証スキーム



①CSMS認定基準:
CSMS認証を行う認証機関に対する要求事項
②CSMS認証基準:
制御システムのセキュリティマネジメントシステムの要求事項
③CSMSユーザーズガイド:
CSMSを構築する組織がCSMS認証基準の理解を深めるために活用するガイド

CSMS認証基準の策定・評価

□ CSMS認証基準の策定経緯

・CSMSパイロット認証用の認証基準として、CSMS認証基準(0.8版)を策定

■IEC 62443-2-1:2010とISO/IEC 27001:2005の差分分析及びIEC 62443-2-1:2010をベースとした認証基準についても検討

■パイロット認証で用いる規格として、現在制御システムセキュリティの国 際規格として策定されているIEC 62443-2-1:2010をベースにCSMS認証基準を検討

■IEC 62443-2-1:2010の要求事項のshallとshouldの扱い方、リスクアセスメントよる管理策の選択の可否等を検討し、CSMS認証基準(0.8版)を策定・評価

CSMS認定基準の策定・評価

□ CSMS認定基準の策定経緯

・CSMSパイロット認証用の認定基準として、CSMS認証機関認定基準及び指針(0.8版)を策定

■CSMS認証機関認定基準及び指針は、マネジメントシステム共通で使用されるISO/IEC 17021:2011をベースにし、CSMS固有の要求事項を検討

■CSMS固有の要求事項は、ISMSの認定基準であるISO/IEC 27006:2011を参考にし、CSMS認証基準を踏まえて追加

■CSMS認証機関認定基準及び指針について検討し、パイロット認証用の認定基準(0.8版)を策定・評価

パイロット認証の受審組織及び認証機関

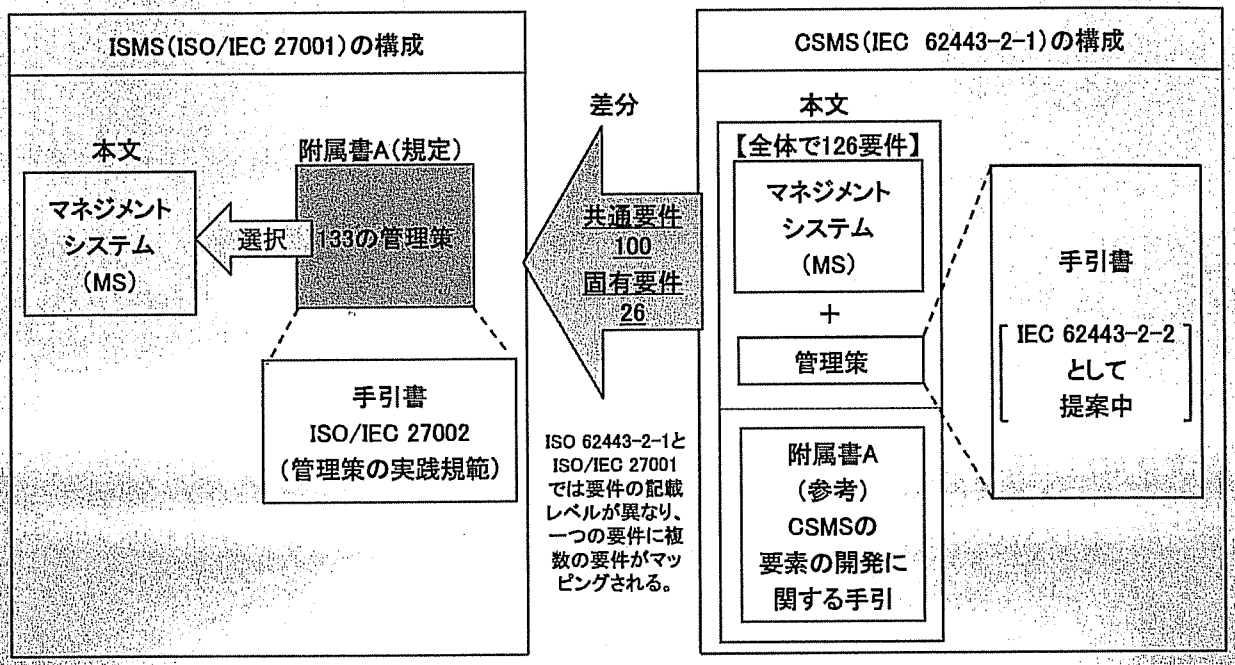
□CSMS認証スキームを確立するため、パイロット認証を通じてCSMS構築・運用を実証する。

■CSMSパイロット認証の実施のため、受審組織の公募を実施(5/15)

■受審組織の決定後(5/31)、認証審査を行う認証機関を決定

受審組織	認証機関
三菱化学エンジニアリング㈱	一般財団法人　日本品質保証機構 マネジメントシステム部門(JQA)
横河ソリューションサービス㈱	BSIグループジャパン株式会社(BSI-J)

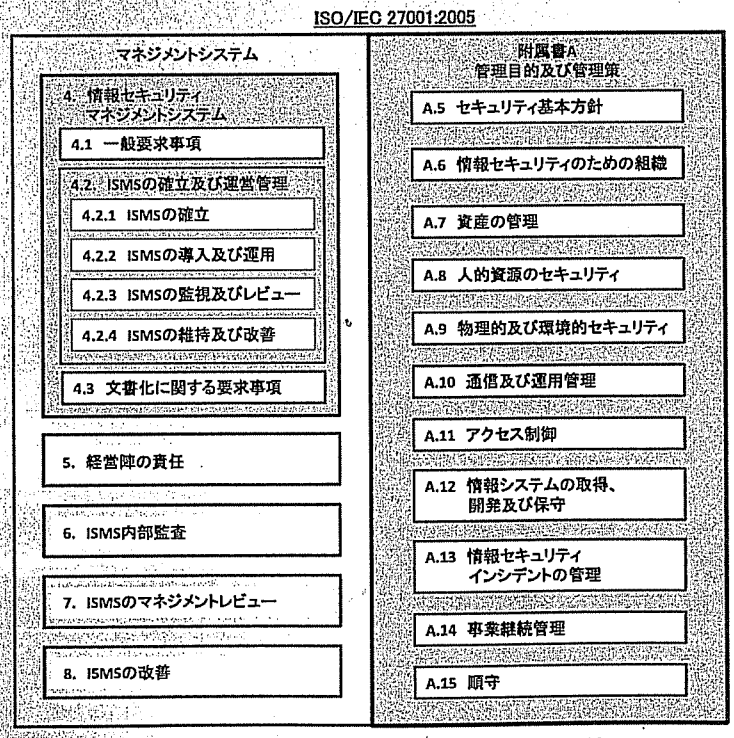
ISO/IEC 27001とIEC 62443-2-1との比較



出典:IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて」2012年10月

15

ISO/IEC 27001の構成



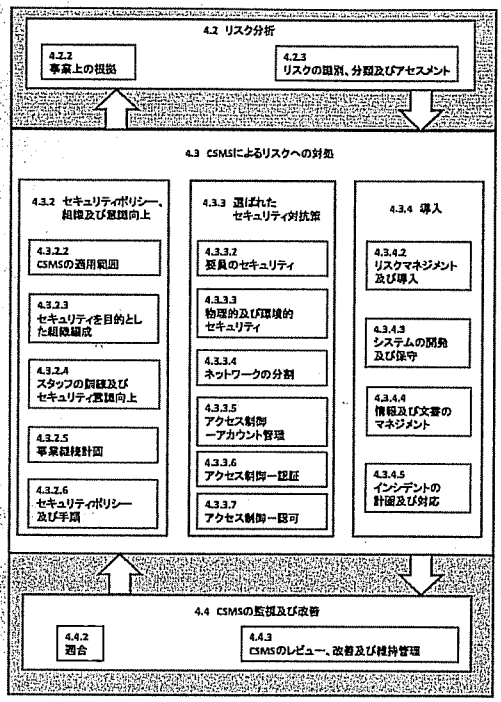
IEC 62443-2-1の要求事項のうち、管理策と関連が強いものが多いと思われる。

マネジメントシステム本文についてもいくつか関連がある。

組織の制御システムセキュリティを強化していくためには、ISMSのマネジメントシステム部分を活用して、組織的に運用していくことが重要と思われる。

16

IEC 62443-2-1の構成



一般要求事項

組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化したCSMSを確立、導入、運用、監視、レビュー、維持及び改善しなければならない。CSMSに要求されている要素はIACSをサイバー攻撃から保護するためである。

CSMSの普及に向けて

□制御システムセキュリティの向上には、CSMS認証が普及して、制御システム事業者が認証取得する流れを確立することが有効であり、制御システム分野のセキュリティレベルの向上につながるものと考えられる。

- ■CSMSの周知と人材の育成
- ■CSMS認証スキームの確立
- ■認証取得に関するコスト負担の軽減
- ■認証取得に対する事業メリットの明確化

出典：IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて」2012年10月

今後のスケジュール

- CSMSパイロット認証の実施
- CSMS認証基準の見直し
- CSMS認証機関認定基準及び指針の見直し
- CSMS審査側の審査上の技術報告のまとめ
- CSMS受審側の構築・運用技術報告のまとめ
- CSMS制度上の課題の整理と解決策の提示
- CSMSユーザーズガイドの公表
- CSMSパイロット認証結果の報告（東京/大阪）

CSMSの普及促進

今後も、様々な活動を通じてCSMSの普及促進に努めます。
皆様方のご支援、ご協力をお願いいたします。

【お問い合わせ先】
一般財団法人日本情報経済社会推進協会
情報マネジメント推進センター

URL: http://www.isms.jipdec.or.jp/

企業組織に迫りくるセキュリティ脅威への備えと対策

一般社団法人 JPCERT コーディネーションセンター
理事　分析センター長
真鍋 敬士

制御システムセキュリティカンファレンス 2014

企業組織に迫りくる セキュリティ脅威への備えと対策

2014年2月5日（11:30-12:00）

JPCERTコーディネーションセンター
理事・分析センター長　真鍋　敬士

本日お話ししたいこと

最近のサイバー攻撃例

インシデントへの対応

サイバー攻撃事例

- サイバー攻撃事例 -

ある日…

製造業の株式会社αからJPCERT/CCにインシデント情報の提供
- ✓ ネットワーク監視サービスで不審な通信の報告
- ✓ 乗換検索サイトβにアクセスした際に感染
- ✓ 感染したマルウエアに関する情報を提供

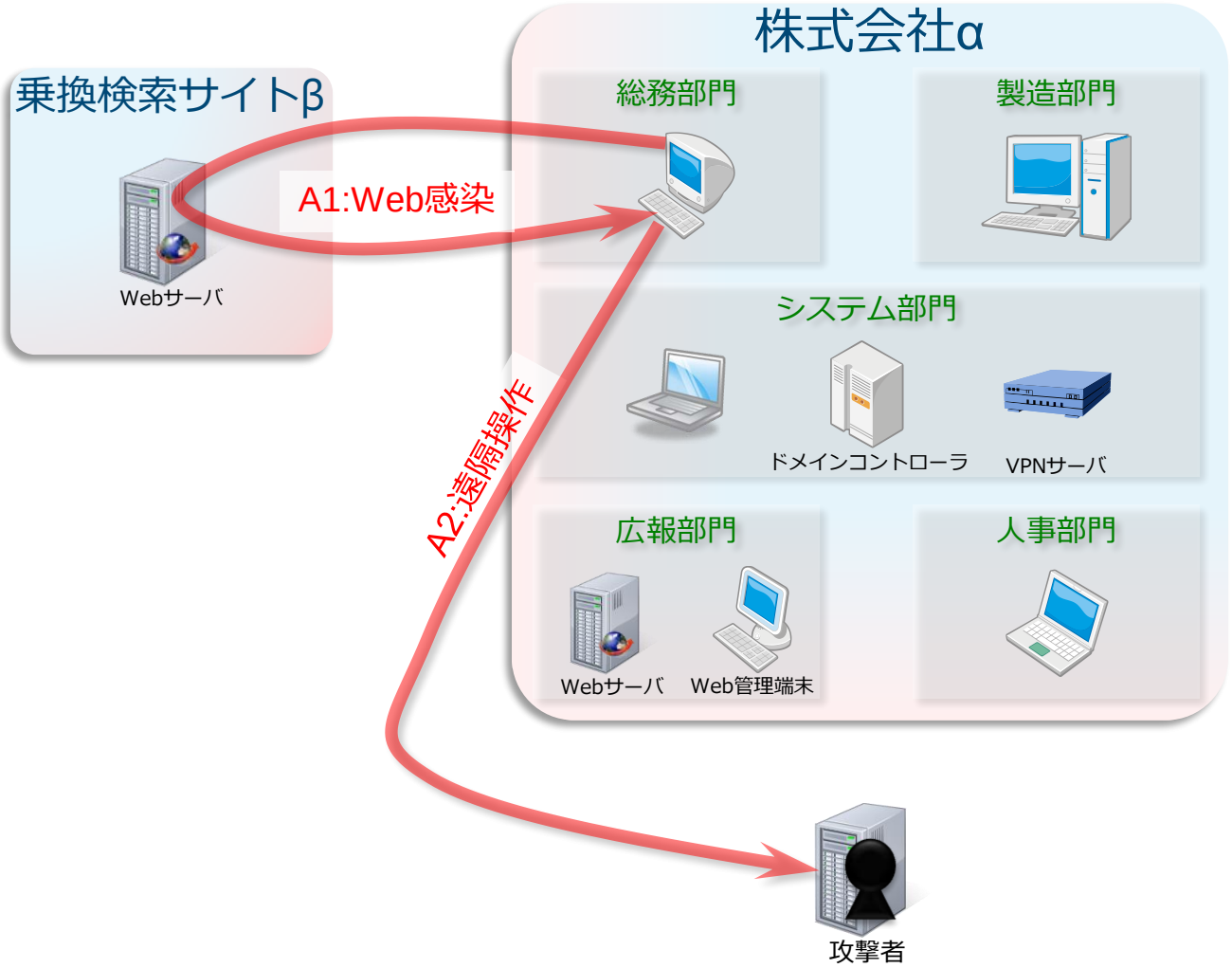
一見すると
ウェブ改ざん

侵入型の
マルウエア

乗換検索サイトβを運営する組織に情報を提供

当該ウェブや不審な通信先に関する情報を展開

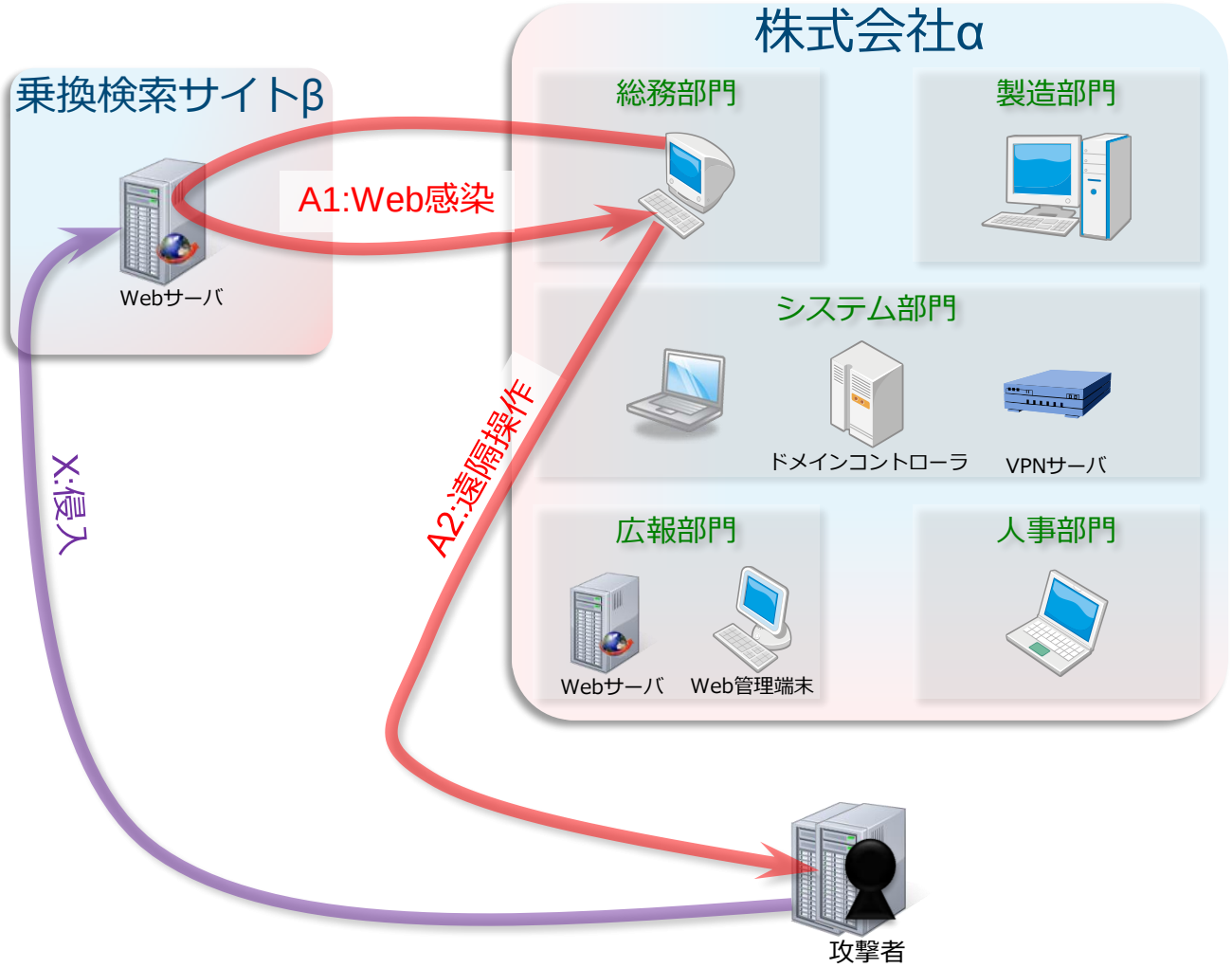
1日目：αからの最初の情報提供



【αでの調査】

- 総務部門のPCが不審なサイトに通信していた。
- ファイアウオールでサイトへの通信をブロックした。
- 当該PCを隔離して調査した。
- βにアクセスした時にマルウエアをダウンロード・実行させられていることが判明した。
- βへのアクセスは日常業務で、直前までは異常なかった。

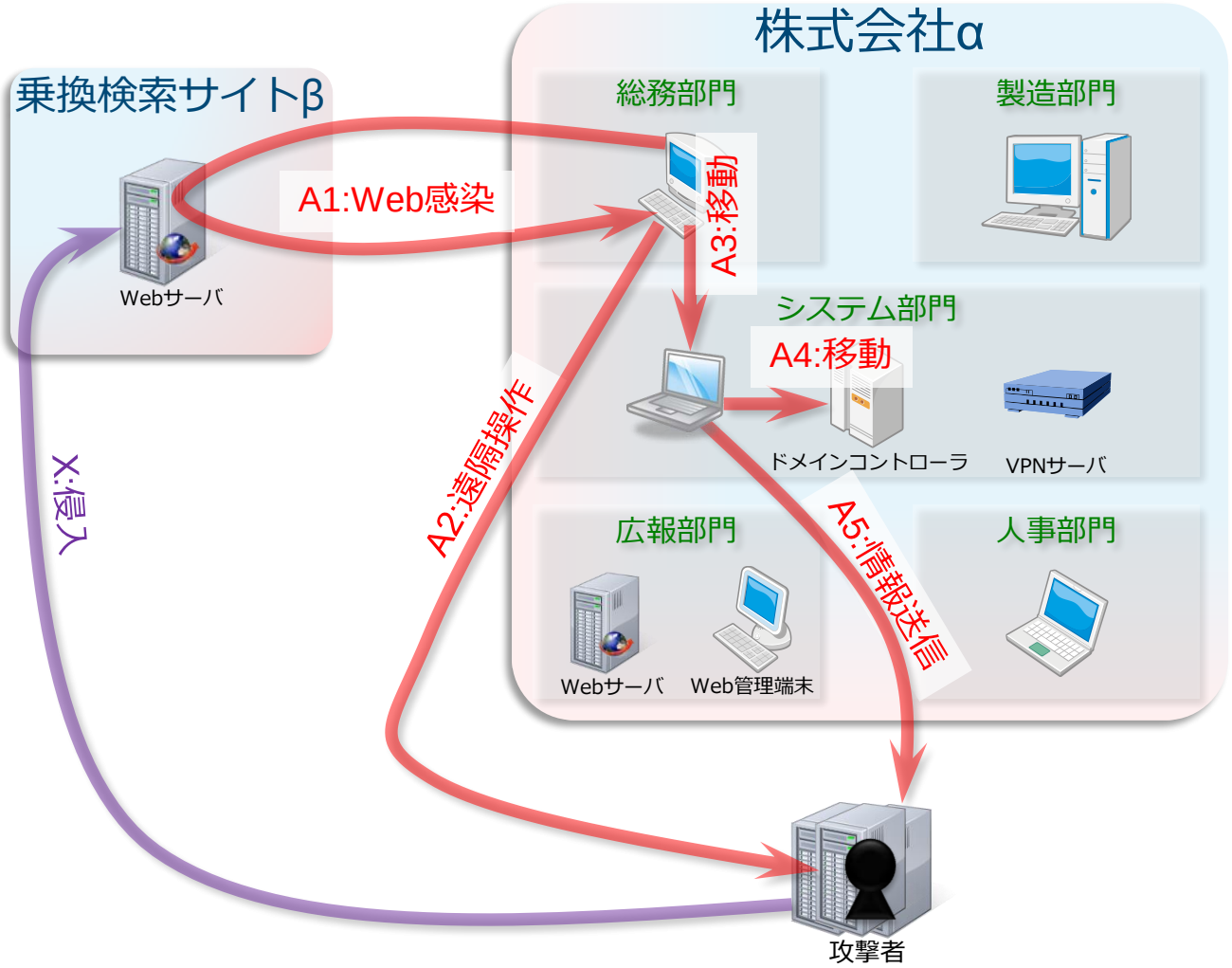
2日目：βからの情報提供



【βでの調査】

- 1ケ月前に外部から侵入されていた。
- 特定のアクセス元に対して不審なサイトへリダイレクトする設定が追加されていた。

2週目：αからの追加情報提供

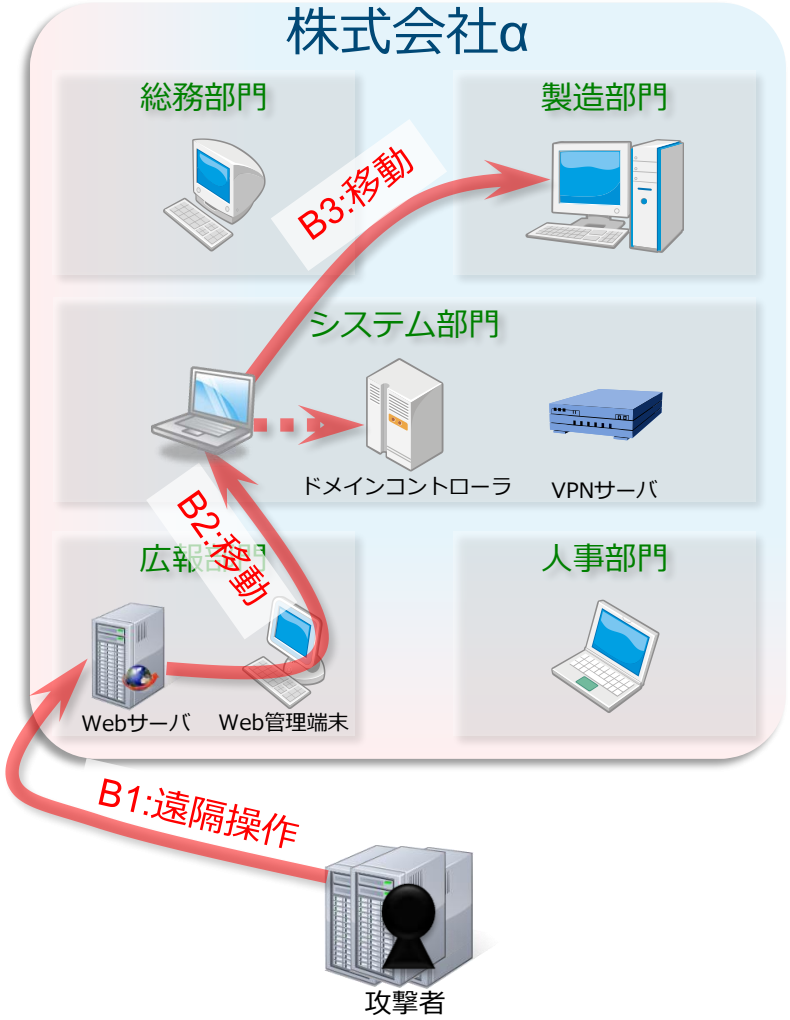


【αでの調査】

- 管理用PCとドメインコントローラに侵入されていたことが判明した。
- 管理用PCから不審なサイトに情報送信された痕跡があった。
- ファイアウオールでサイトへの通信をブロックした。
- 全アカウントのパスワードを変更した。

3週目：αからの情報提供（再侵入）

【再侵入の調査】
- ドメインコントローラへの侵入の試みを検知した。
- Webサーバから Web管理端末と管理用PCを経由して侵入を試みていた。
- 製造部門のPCにも侵入されていた。
- 前回の侵入時にWebサーバとWeb端末に裏口が設置されていた。



前回の侵入に対して
関係部門のみ
（総務とシステム）
で対応を進めていた

全社を対象に調査

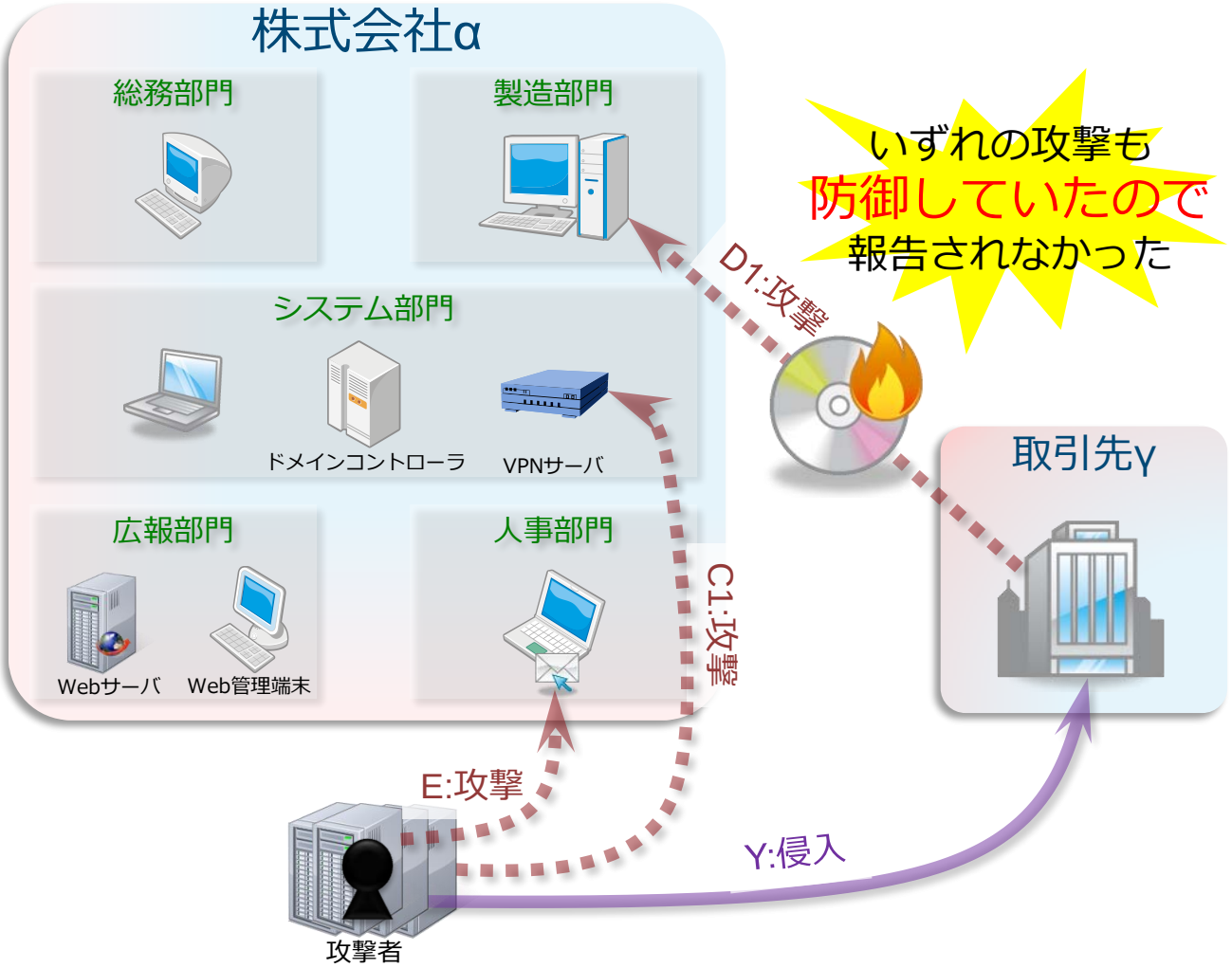
4週目：αからの情報提供（全社調査結果）

【人事部門】
先週から不審なメールが何通も届いている。

【システム部門】
先々週からVPNサーバへの不審な接続試みが続いている。

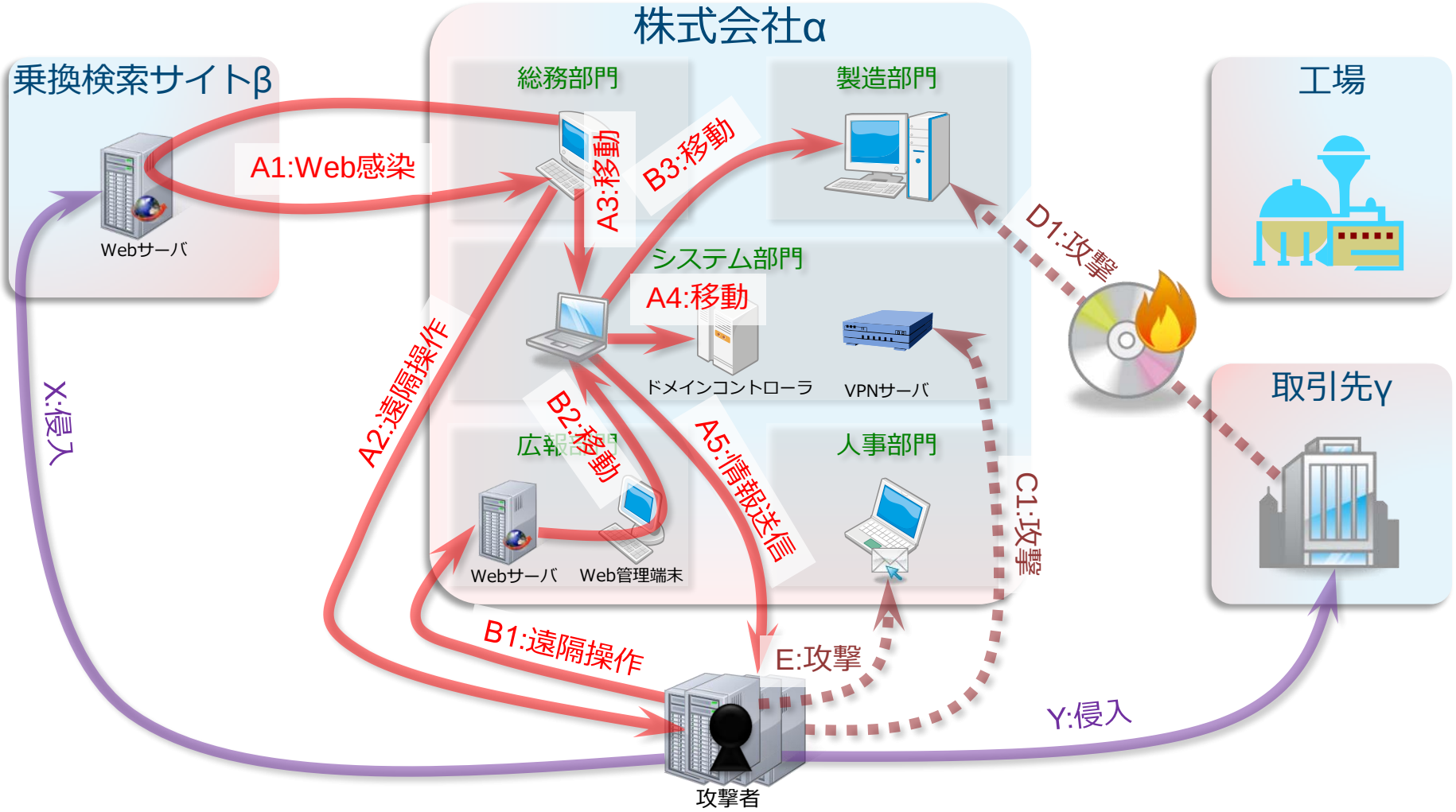
【製造部門】
先々週にマルウエアが混入したDVD-Rが届いていた。

【取引先γ】
6ヶ月前に外部から侵入されていた。



攻撃の全容

他組織も巻き込んで**様々な手段**で**次々**と攻めてくる…



インシデントへの対応

取組みから見た「二つの脅威」

使われる技術や手段には共通性もある
成果がやりとりされている可能性もある
でも、簡単に見分けられるとは限らない

- 直接的な被害をともなう
- 短期間で行われる
- 変化しながらも単純に繰り返される

- 被害がわかりにくい
- 必要に応じて長期間かけて行われる
- 様々な手段で継続的に繰り返される

守りを固めて排除する ⇔ 対応の違い ⇔ 観察して避ける

- インシデントへの対応 -

対応プロセス

マネージメントの積極的関与

外部との情報連携

外部からの情報で
インシデントが発覚する
ケースが多い

攻撃を特徴づける情報

ここが
最も重要

一般的に
ここが起点になる

外部と共有

準備 → **検知・分析** → 封じ込め → 根絶 → 修復 → 教訓

役立つのは…
- ✓通信ログ（ファイアウオール、プロキシ等: 内部⇒外部や内部⇒内部）
- ✓証跡データ（端末ログ、IT資産管理システム等）
- ✓IT資産管理情報

※ログ類は状況により6カ月～1年以上遡る

平常時の備え

有事における対応

侵入事例での対応を振り返る

- 早く全社調査していればWebサーバやWeb管理端末の裏口を発見・駆除できていたかもしれない。
- 全社調査が遅くなれば、再々侵入を許していたかもしれない。

再侵入を防ぐことはできなかったのか？

被害は何だったのか？
攻撃者の狙いは？

- ユーザや端末の情報以外にもデータを持ち出された可能性はあるが内容は特定できていない。
- 他の組織や工場が本来のターゲットだった可能性もある。

- 様々な手段で攻撃が繰り返される。
- 継続的に観察できることが対策に繋がる。

終息宣言は？

想定される被害は？

- 情報漏えい
  - 注目されるのは個人情報の漏えい
    - 「攻撃者はあらゆる情報に価値を見出す」と考えるべき
  - 盗まれた情報を完全に特定することはほぼ不可能
    - 全ての情報アクセスと全ての通信を記録する必要がある
    - 盗まれることを前提に情報を無効化するという考えも
- インフラの乗っ取り
  - サプライチェーンに対する攻撃の温床
    - 「自組織には盗まれて困る情報はない」という思い込み
  - 自爆的な攻撃
    - インフラを使って攻撃メールを派手にばらまく
    - 取引先やメディアへの対応に翻弄される
- 対応のために発生したコスト
  - サーバ・端末、ログ類の調査費用
  - サーバ・端末の調査・復旧にともなう業務停止

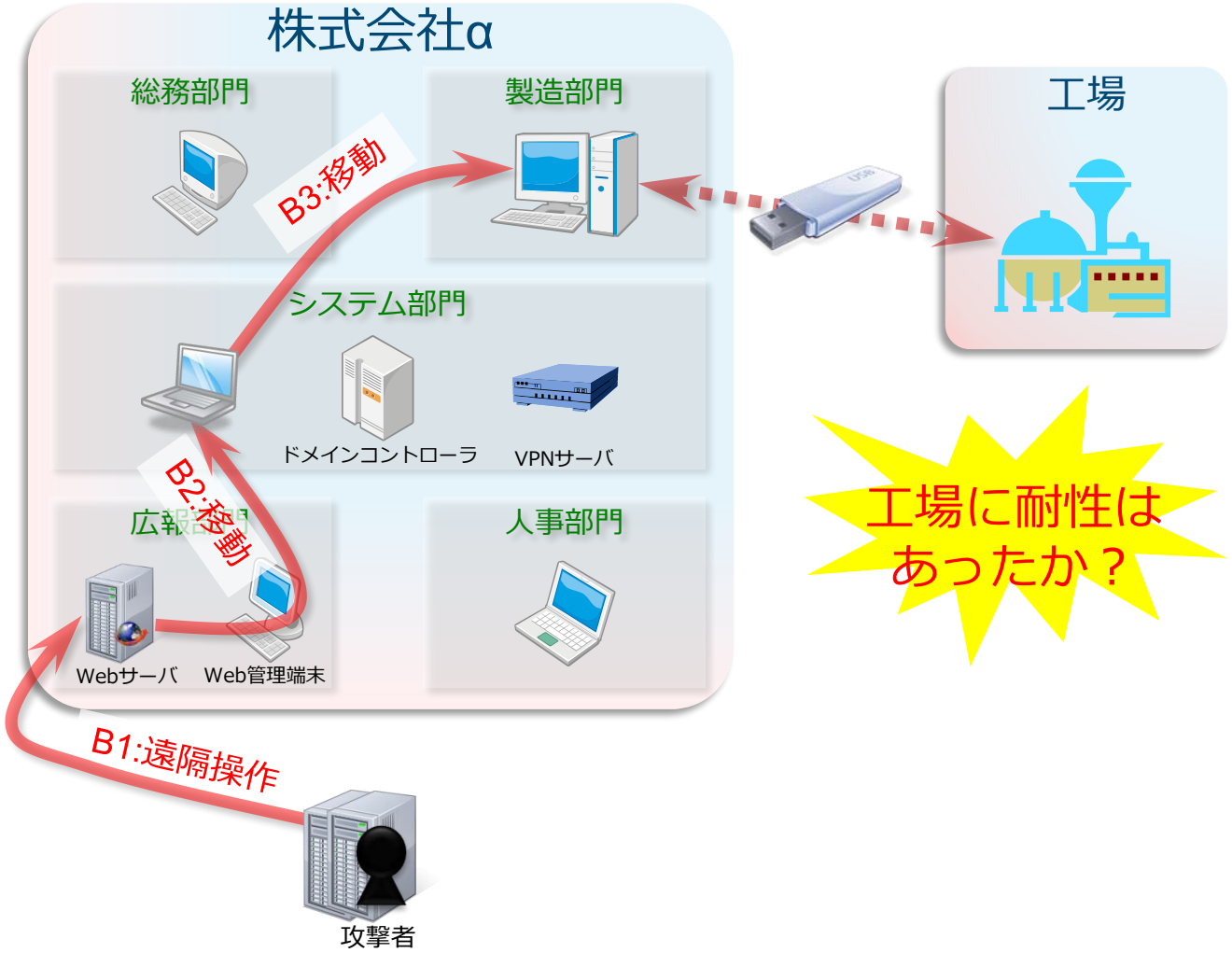
外部への情報発信時の焦点になりやすい問題

当事者になって初めて思い知らされる問題

発覚後に捻出しなければならない費用

もし工場がターゲットだったら…

【工場】
正常部門との間でUSBメモリを使ってデータのやりとりをしている。



脅威への対応と対策

事後対応

- 緊急対応体制の起動
  - 組織内の統制
  - 対応スケジュールの検討
- サーバ・端末やログ等の調査
  - 侵入経路や影響範囲の特定
  - クリーンナップ
- 外部への情報発信
  - 二次被害の危険性のある対象への注意喚起
  - メディア等への対応
  - セキュリティベンダ等への情報提供

ゼロからの対応は困難

事前対策

- 情報集約と情報連携の取組み
  - CSIRT機能の構築
  - 情報連携の取組みへの参加
- 攻撃との共存を意識した環境作り
  - セキュリティ教育・トレーニング
  - ログ設定のチューニング
  - メールのアーカイブ・検索
  - 次世代ファイアウォール等の導入検討
- 情報資産の把握・保護
  - ネットワークやシステムの構成把握
  - 保護すべき情報の洗い出し

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。

ICS Security Enhancement in the National Control Centers of Taiwan Power Company

台湾電力公司 (Taiwan Power Company)
Deputy Director System Operation Department
Mu-Chun Chang

ICS security enhancement in the national control centers of Taiwan Power Company

Chang, Mu-Chun
Deputy Director
Department of System Operation
Taiwan Power Company(TPC)

Outlines

- ✓ Control Centers' Structure of TPC
- ✓ System Configurations Of The NCCs
- ✓ Computer Security Issue
- ✓ Security Enhancement
- ✓ Conclusion

Control Centers' Structure of TPC

- Redundancy of Control Center—Dual Primary CC
  - The CS in two control centers operate as primary system
    (Note: The APP like **AGC** at Taipei can be set as *active* mode, Kaohsiung site's AGC needs to be set as *blocked* i.e. listen mode)
  - They can operate simultaneously and backup each other
  - The CS in two control centers can operate in stand-alone mode
  - Links' back-up between CCs and remote sites is flexible
- Backup of Control Centers—Security Consideration in CC Level
  - Two provisional CCs can be set-up for Taipei and one provisional CC for Kaohsiung if necessary

Control Centers' Structure of TPC

Taipei National Control Center (NCC)

Taipei Provisional CC #2

Taipei Provisional CC#1

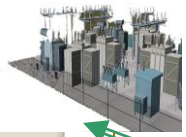
SIEMENS System

EHV Substations

Control /Data

Control /Data

Power Plants



基隆 ADCC

台北 ADCC

新桃 ADCC

台中 ADCC

嘉南 ADCC

高雄 ADCC

K.L.-Area DDCC

T.P.-Area DDCC

S.T.-Area DDCC

T.C.-Area DDCC

C.N.-Area DDCC

K.S.-Area DDCC

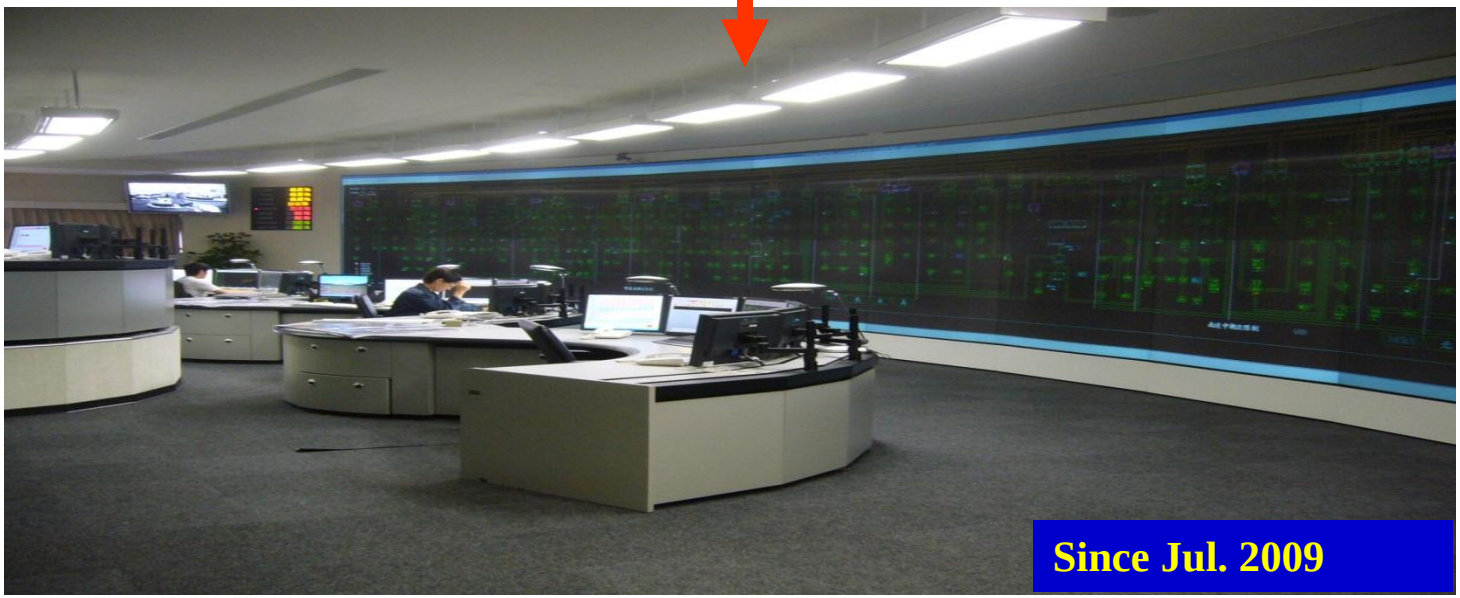
SIEMENS System

Kaohsiung NCC

Kaohsiung Provisional CC

Taipei & Kaohsiung NCCs

Since May 2010



Since Jul. 2009

System Configurations of The NCCs

- Redundancy of Computer System—Security Consideration in CS

  EMS/SCADA computers have traditional redundant scheme

- Back-Up system for SCADA

  Dispatchers can still use a standalone SCADA system when all EMS/SCADA of Taipei and Kaohsiung NCCs fail

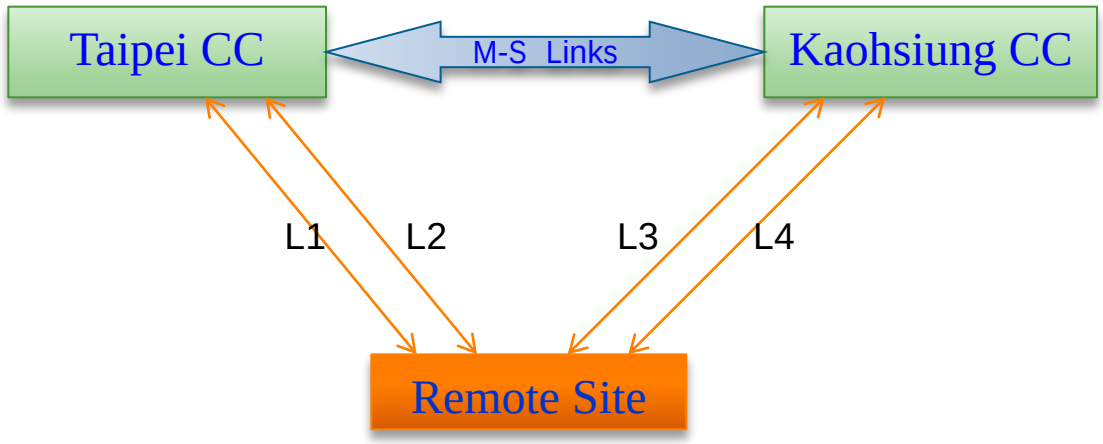
- Redundancy of Network Telephone System

  Network Telephone System has redundancy capability for every component from servers to corporate com. lines

- Back-Up system for Network Telephone System

  2 traditional(micro-wave and telecom.) telephone systems will be used when the Network Telephone System fails

Links' back-up

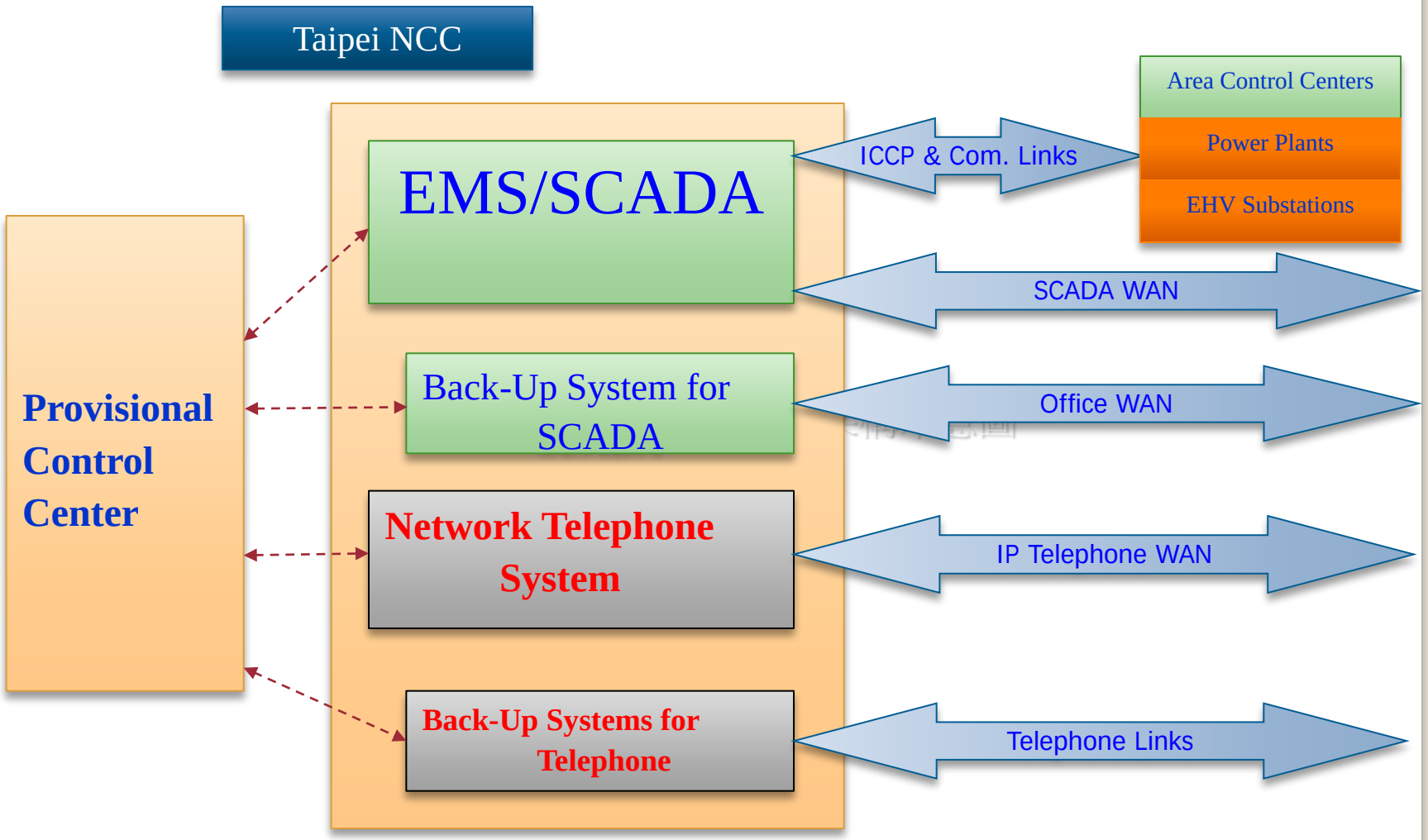


If **Taipei CC** is DR(Data Responsive) Mode for a particular Remote Site, **Taipei** sends Data received from **Remote Site** to **Kaohsiung** thru **M-S Links**

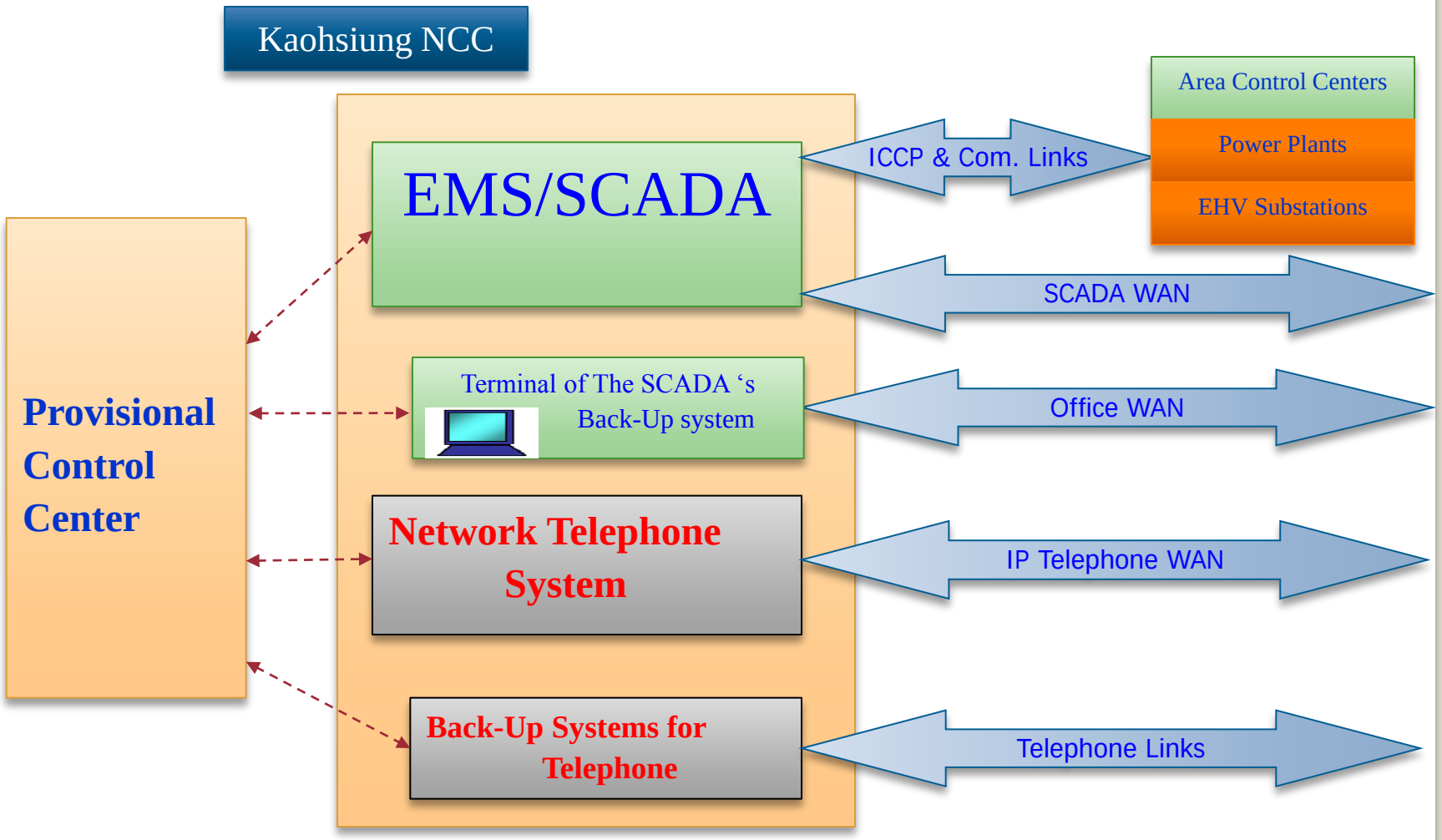
(Note: Kaohsiung can be set as DR mode)

Taipei CC is at DR Mode,
if **L1** fails, **L2** takes over
if both **L1** & **L2** fail, **L3** or **L4** takes over

System Configuration Of The NCCs p.1/4

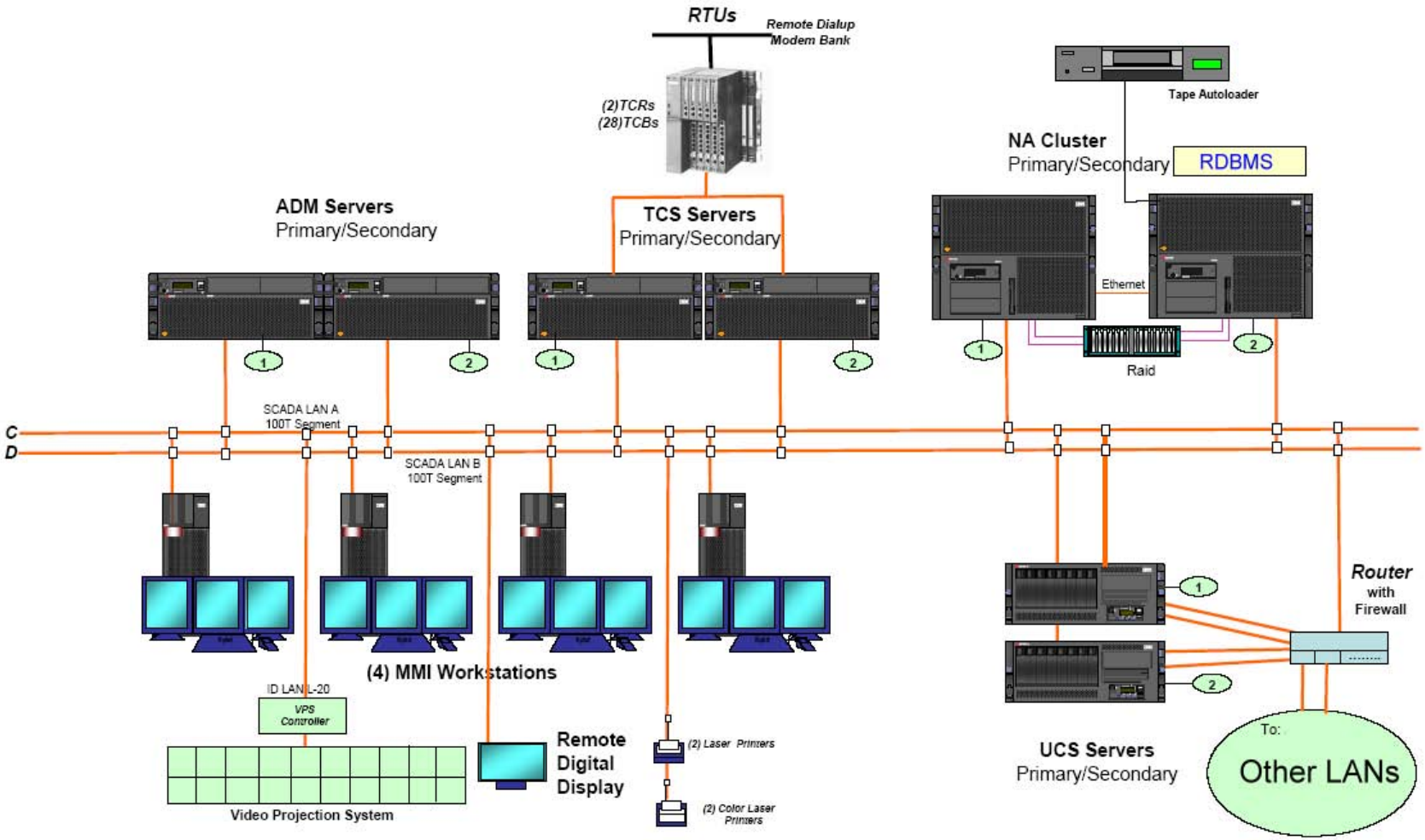


System Configuration Of The NCCs p.2/4



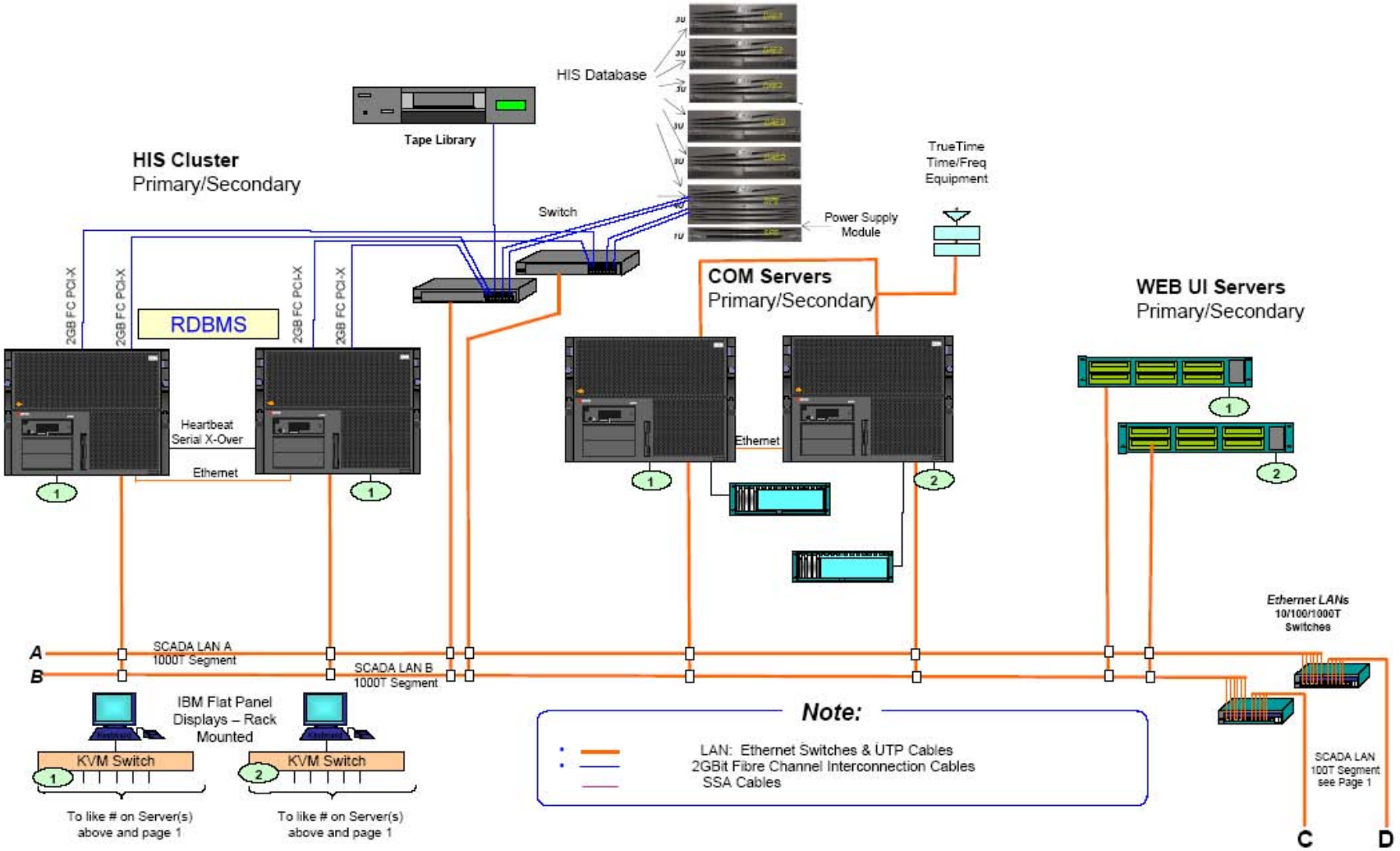
System Configuration Of The NCCs p.3/4

EMS/SCADA (p.1)



System Configuration Of The NCCs p.4/4

EMS/SCADA (p.2)



Computer Security Issue

- Invulnerability Control

  ICS structure design– Dual primary control system gets higher reliability

  Provisional CCs– Dispatchers can still use CS in special events such as SARS (Severe acute respiratory syndrome) break out

  Backup systems of CS and Telephone System– Malfunctions are also considered

  Communication media– ICS uses non- public com. lines and networks to prevent cyber attacks and every link is equipped with backup

  Remote access to ICS– Only vender's engineers can access ICS from remote site after permission

Computer Security Issue (cont.)

- Incidents encountered

  Nature disaster caused ICS down– A power line tower fell down due to an earthquake, the high speed com. links carried by an OPGW over that tower broke, then ICS and its Back-Up System crushed and re-started

  Adding code caused ICS blind– All MMI monitors became blind after ICS re-start because an engineer failed to thoroughly test before adding code

  Special Protection System (SPS, an external stand-alone system used by dispatchers) seemed to receive attacks by a Trojan Horse

Security Enhancement

- Enhancement in ICS communication medias

  Good lesson was given from the event that nature disaster caused ICS down – using different media types for backup

- Disciplining engineers in system maintenance work

  ICS changes such as adding code must be thoroughly tested first then get approval by managers

- Upgrade OS when necessary

  External system such as SPS needs to be upgraded frequently to make sure completed hotfix and software patches are in place

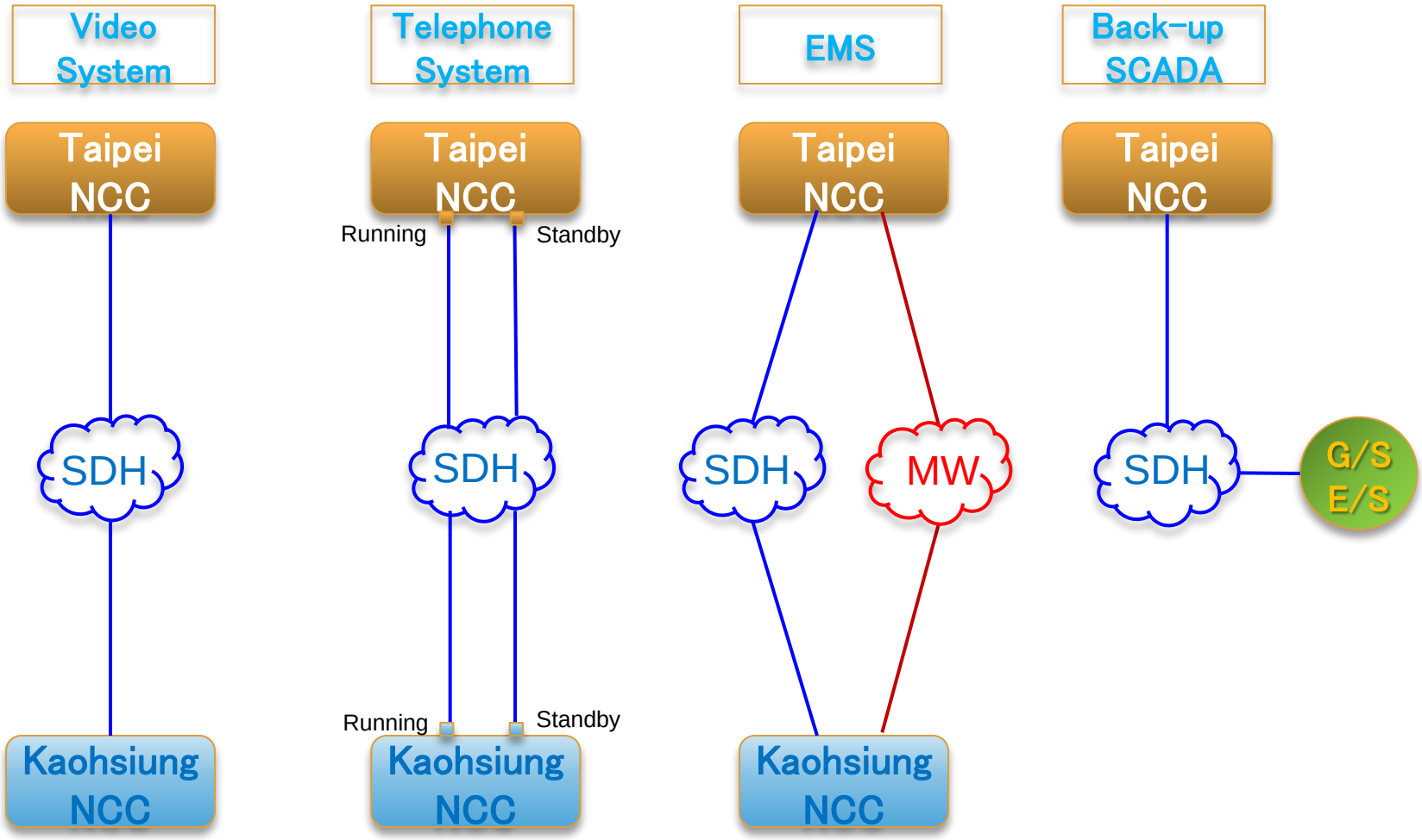
- CS's firewalls can be further protected

  The firewalls of CS can be monitored by the Security Operation Center (SOC) set up by IT department

Security Enhancement (cont.)

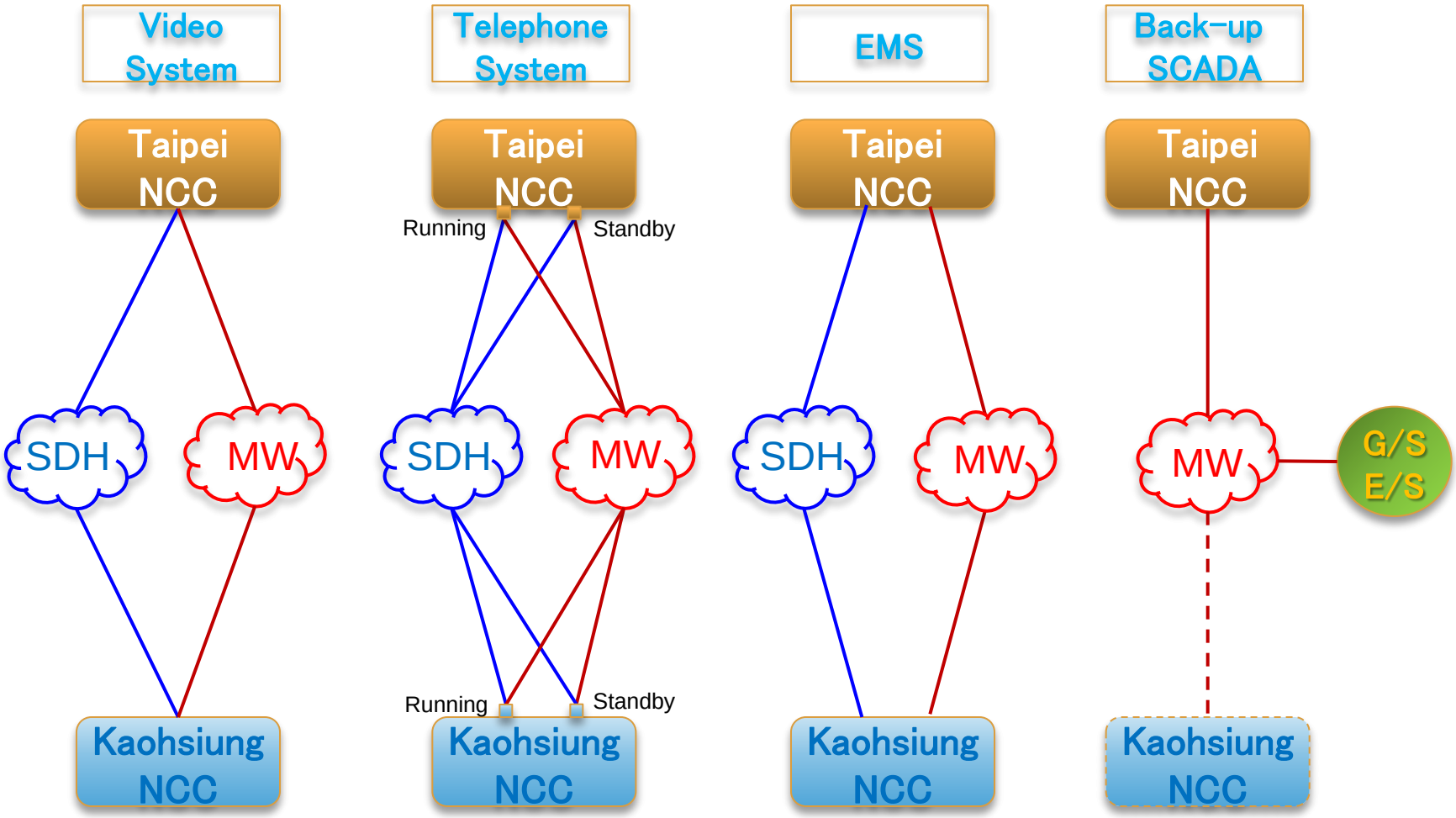
- More critical power plants and EHV stations were added to Back-Up System for SCADA after participating CIIP drills conducted by a government agent
- To Set up Back-Up System for SCADA at Kaohsiung NCC

ICS Comm. Media (Original)



SDH：Synchronous Digital Hierarchy
MW：microwave

ICS Comm. Media (Improvement)



SDH：Synchronous Digital Hierarchy
MW：microwave

Conclusion

- Electric power supply is considered as important as national defense level
- Both ICS and telephone systems of TPC's NCCs are crucial to power-dispatch
- The security enhancement work in ICS and telephone system began from systems' start-up and never stops
- TPC's NCCs needs to sustain operations in danger of bird-flu(e.g. H1N1-virus pandemic) or cyber-attack
- So, TPC needs to train dispatchers to use the provisional CC's facilities often and to collaborate with government in various cyber-attack drills for the CIIP plans

Thank you
for your attention!

Taiwan power company

Management Philosophy:
Integrity Caring Innovation Service

The Kaizen of ICS Security

The Langner Group
Co-Founder and Managing Principal
Ralph Langner

Ralph Langner
The Langner Group
Arlington | Hamburg | München

The Kaizen of ICS Security

Old-School (Western) ICS Security Wisdom

Paradigm:
Risk Management

Langner

ICS Risk Management

in four easy steps

1. Do nothing for a couple of years

2. Assess risk. No credible threats? GOTO 1.

3. Risk „acceptable“, or mitigation too expensive? GOTO 1.

4. Mitigate the risk you know about (and nothing else) for minimum cost, preferring technical gizmos. GOTO 1.

Langner

ICS Risk Fundamentals

1. A threat-driven approach cannot look farther than the predictability window of threats.

2. Lead time in ICS environments is measured in years.

3. New threats and vulnerabilities may pop up at any time.

Langner

Risk-based School of Thought

Event-driven:	Focus on outside factors that cannot be controlled (→ threats)
Non-empirical:	Use of parameters that cannot be measured (example: attack probability)
Biased:	Fixation on IT components and technical point solutions that only address part of the problem

New-School (Kaizen) ICS Security Wisdom

Paradigm:
Continuous Improvement

Langner

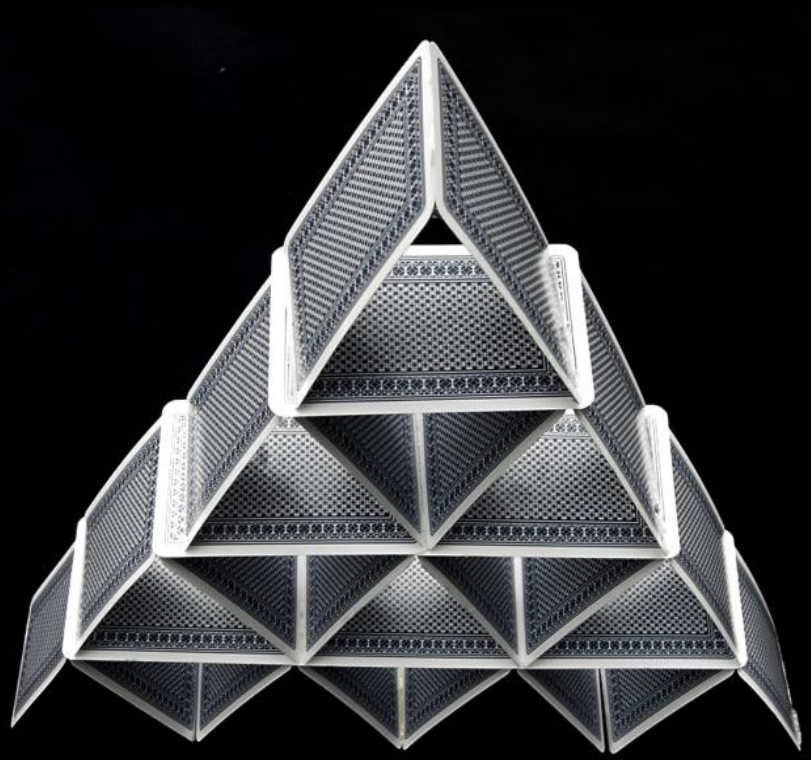
Kaizen: Focus on
- solutions,
- internal factors that we can control,
- systems and processes in context
- long-term improvement

Risk & Threat: Focus on
- the magnitude of the problem,
- external events to which we try to respond,
- components in isolation (single out hot spots)
- short-term trouble control

Security as a property of process control

Process control is insecure (or fragile) to the extent that *more things can happen than planned*

→ Lack of predictability and robustness in systems and procedures



What are relevant threats to this object?

Langner

Taguchi on Quality

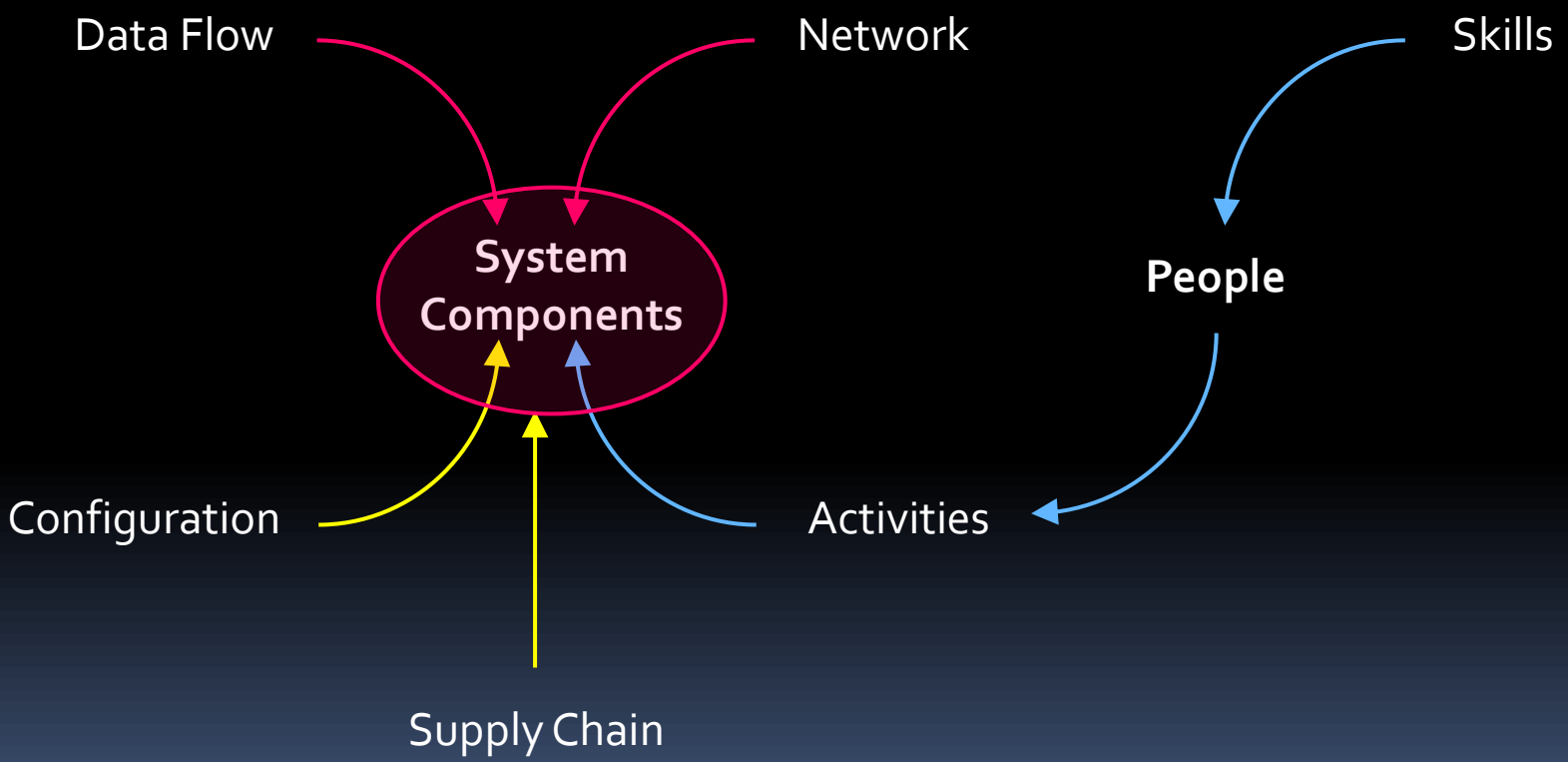
„Quality is evaluated by quality loss, defined as the amount of functional variation of products plus all possible negative effects, such as environmental damages and operational costs.“

Langner on ICS Security

„ICS Security is evaluated by loss of predictability, defined as the amount of functional variation of process control plus all possible negative effects, such as environmental damages and operational costs."

Langner

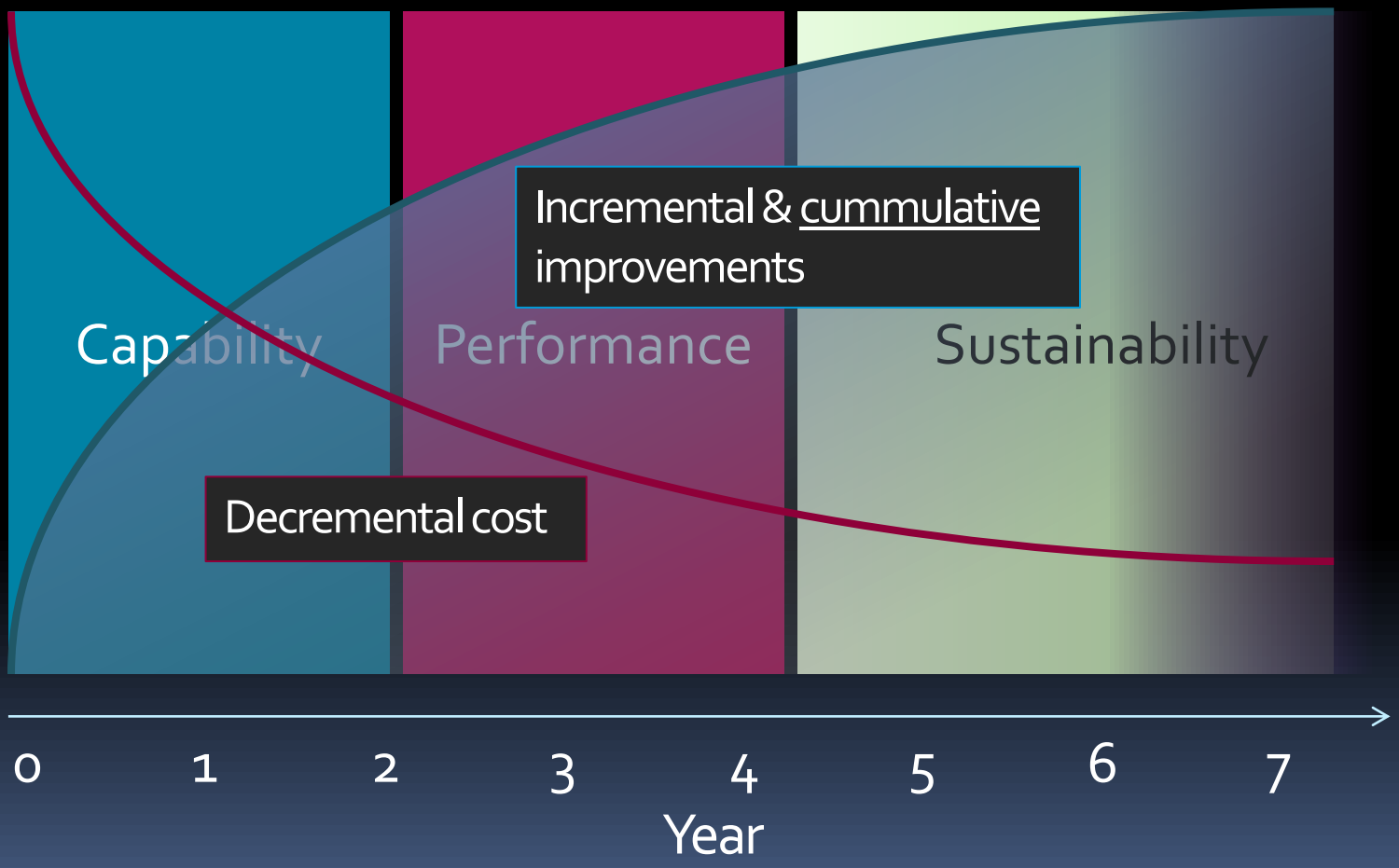
360˚View: Factors that we can control



ICS Insecurity Markers

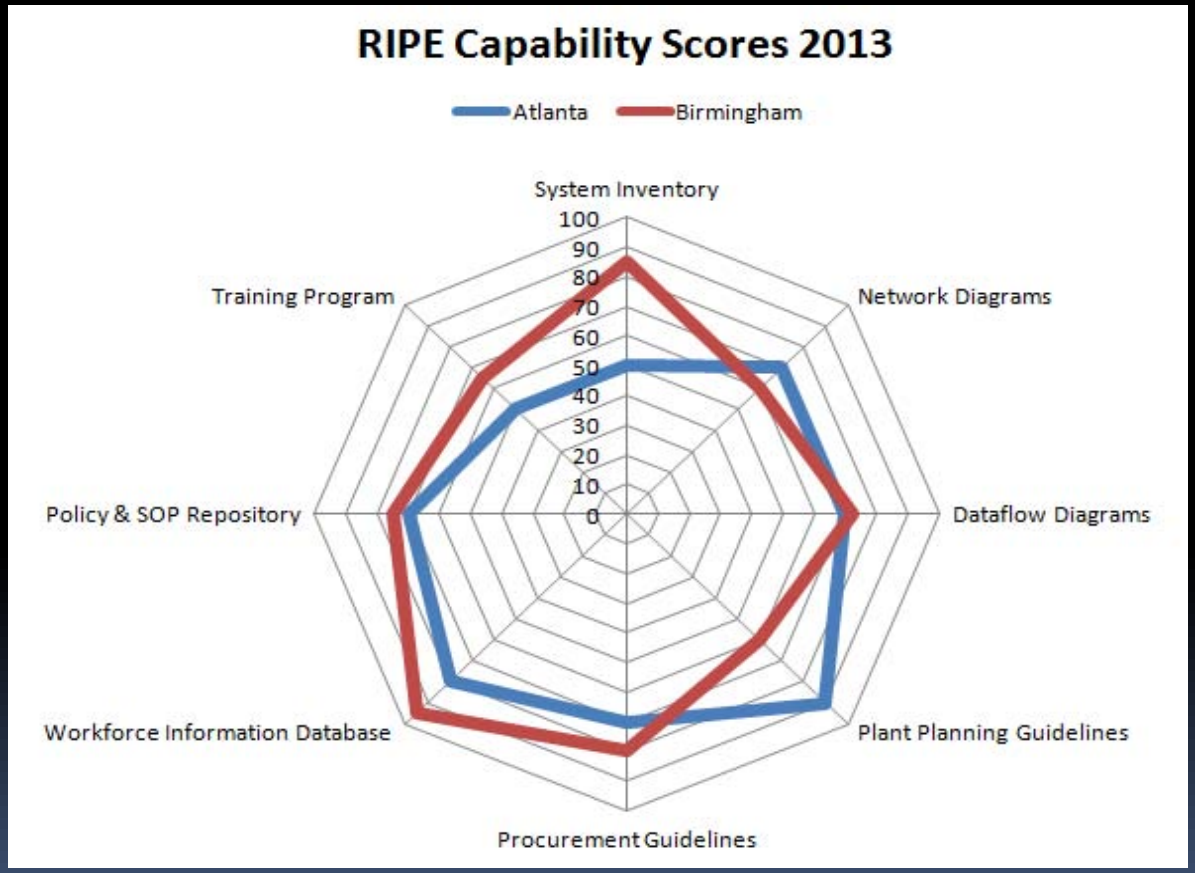
1. You don't know exactly which control systems are used in your plant, and their respective versions and configurations
2. You don't know the exact data flow and dependencies between components
3. You have inaccurate network diagrams that end at the switch level
4. You don't control your supply chain
5. You don't know exactly who your contractors are that access your ICS
6. You don't enforce security policies
7. You don't systematically train your workforce in ICS security
8. You don't have clear guidelines for control system design and architecture

Continuous Improvement



Langner

Capability metrics & benchmarks



Langner

Recommended Reading

Langner, R.: *Robust control system networks. How to achieve reliable control after Stuxnet.* New York, Momentum Press 2012

Langner, R.: *The RIPE Framework. A process-driven approach towards effective and sustainable industrial control system security.* http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf

Langner, R.: *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve.* http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Langner, R. & Pederson, P.: *Bound to fail. Why cyber risk cannot simply be „managed" away.* http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber%20security%20langner%20pederson/cybersecurity_langner_pederson_0225.pdf

Langner

Q & A

Ralph Langner

The Langner Group

Arlington | Hamburg | München

www.langner.com

ICS Security Enhancement in Australia

CERT Australia
Senior Technical Adviser
Simeon Simes

Australian Government
Attorney-General's Department

February 2014

CERT AUSTRALIA

Control Systems Security

A CERT Australia Perspective

Simeon Simes

Senior Technical Adviser

Topics

- CERT Australia – National CERT
- security environment, implications, controls
- Engaging with CI/SNI owners and operators
  - Briefing on the secruity environment
  - Alerts and Advisories
  - Training
  - Exercises
- Strong regional and international partnerships

Terminology

- CERT - Computer Emergency Response Team
- CI – Critical Infrastructure
- SNI – Systems of National Interest
- TLP – Traffic Light Protocol

CERT Australia

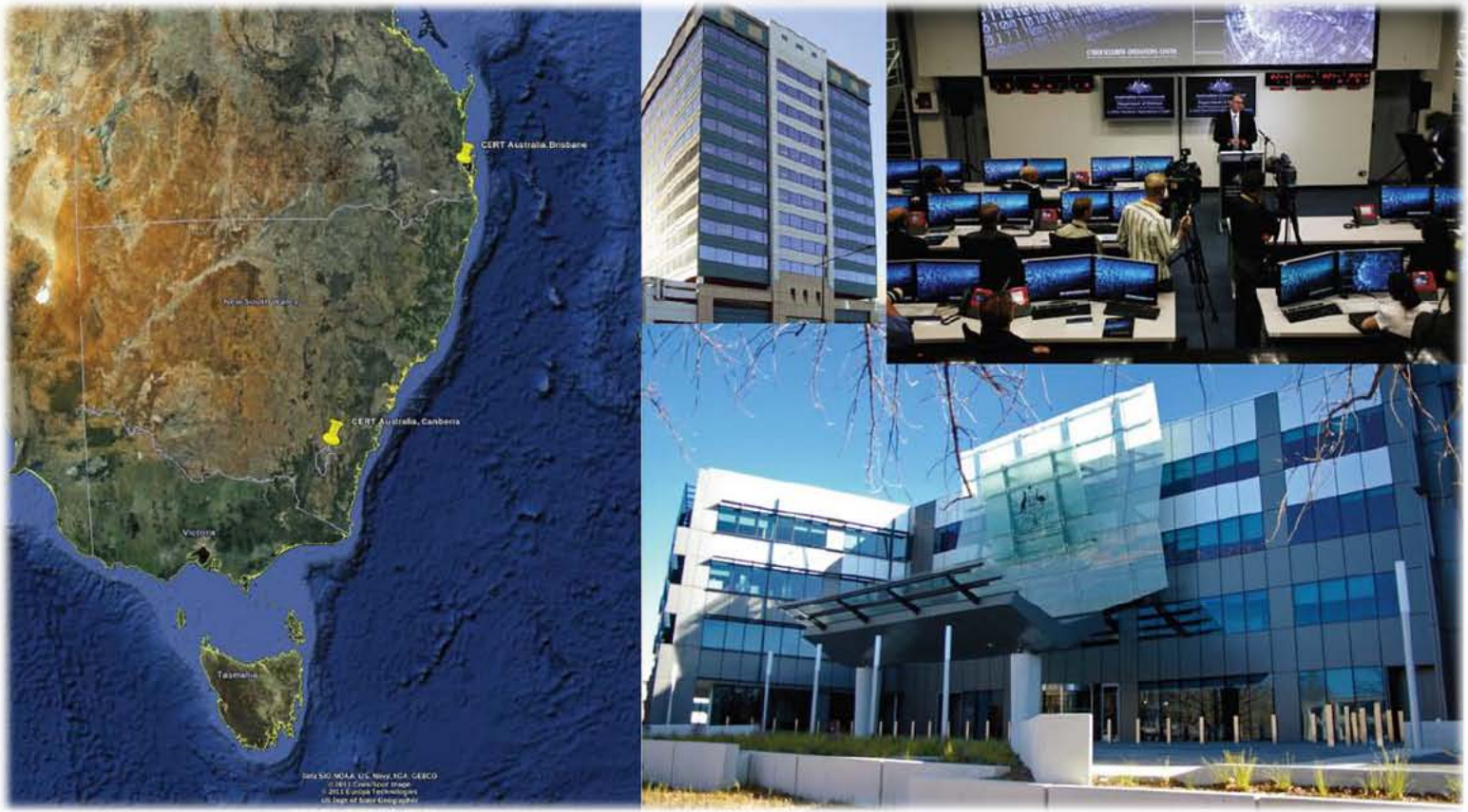
- Australia's national computer emergency response team (CERT)
  - link between industry and government on cyber security
  - Initial point of contact for cyber security information nationally and internationally
- Provide information on cyber threats and vulnerabilities to owners and operators of and systems of national interest (SNI)
- Coordinate technical aspects of a serious cyber event
- Respond to cyber security incidents impacting Australian SNI
- Lead and coordinate collaboration on identifying emerging threats and vulnerabilities (looking ahead)

An Australian Government Initiative

PROTECTING OUR NATIONAL INTERESTS ONLINE

CERT AUSTRALIA

Who is CERT Australia?



The environment, implications and controls

An Australian Government Initiative

The environment

GLEG

NEW: SCADA+ Pack

An effort towards 100% public SCADA vulns coverage

0 Days for SCADA!

Focused on Industrial software & hardware environment

Weak points analyses

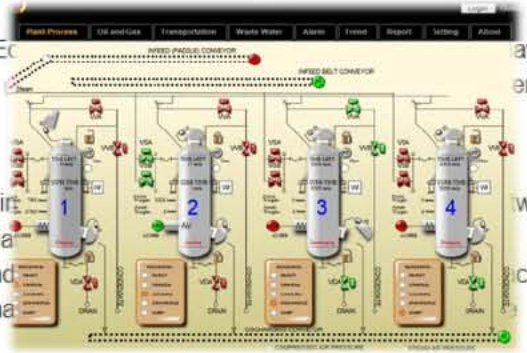
Average Attack Bandwidth up 718 percent;
Average Packet-Per-Second Rate Reaches 32.4 Million According to Prolexic's Q1 2013 DDoS Report
April 17, 2013
Giant attacks overwhelming appliances, ISPs, carriers, content delivery networks

Scada Zero Day released at S4 Conference

Posted by: FastFlux January 19, 2014 in Exploits, Security Leave a comment

Malaysian SCADA computer software organization E[illegible]ay vulnerability in its flagship human machine interface [illegible]ence this week.

The patch repairs a buffer overflow vulnerability within [illegible]ware. HMI application supplies a visualization of commercia[illegible] interfaces contact programmable logic controllers and [illegible]ce, often a Windows-based system. Those processes ma[illegible] control and much more.



CERT AUSTRALIA

The implications

September 2007	June 2010	March 2011	June 2011	September 2011	January 2012
• DHS Aurora demonstration	• Stuxnet	• Auriemma – drops 34 of 58 vulnerabilities in one day	• Metasploit bounty for ICS exploits	• McCorkle and Rios • 100 bugs in 100 days	• Project Basecamp (Digitalbond S4)

Stuxnet 0.5: The Missing Link

Geoff McDonald,
Liam O Murchu,
Stephen Doherty,
Eric Chien

Effective controls

- Threat of disruption and destruction poses significant risk in control systems
- Consequence of compromise of ICS is much more than average corporate system
- Implement effective controls on the corporate and control networks.
  - Protection of corporate well understood
  - Effectiveness of controls used in corporate environment less clear for ICS environment

Government Response

Trusted Information Sharing Network

- The TISN was established by the Australian Government in April 2003
- Forum for owners and operators of critical infrastructure work together and share information on threats and vulnerabilities
- Develop strategies and solutions to mitigate risk.
- The TISN operates on an all hazards basis.
- Comprises seven critical infrastructure Sector Groups and two Expert Advisory Groups.

Sector Groups

Sector Groups form the bridge between government and the individual owners and operators of Australia's critical infrastructure. Their purpose is to assist owners and operators to share information on issues relating to generic threats, vulnerabilities and to identify appropriate measures and strategies to mitigate risk.

CERT engagement

CERT engagement

- Providing security information to SNI owners and operators
  - Alerts and advisories
  - Incident response
- Working with industry and researches
- Exercises
- Training
- Working with regional and international partners

Working with industry

- Provide one-on-one briefings to industry of the threat environment and the effectiveness of controls selected.
- Provide technical guidance on mitigating threats and vulnerabilities, including on system architecture
- Facilitating engagement with others within sectors and in other sectors
- Provide high level architecture guidance and a security sounding board

Advisories / Incident Response

- Advisories on vulnerabilities with an emphasis on providing mitigations
- Advisories with a focus on controls systems vulnerabilities
- Locally relevant information
- Provide advice and assistance during an incident
- Assist in mitigating threats and vulnerabilities

Information Exchanges

- It enables business and government to exchange highly sensitive cyber security operational information in a trusted environment
- Technical specialists from a broad range of SNI
- Share information to gain an understanding of common threats and mitigation strategies
- Participation by a wide range of sectors , industries, and other agencies

Cyber Security Exercises

- Assisting owners and operators of CI/SNI with cyber security exercises
- Local and international
- Design and development
- Active participant
- Outcomes

Training

- Provision of training opportunities to owners and operators
- Australian universities
- CERT an active contributor
- Outcomes

Queensland University of Technology

CONTROL SYSTEMS: CYBER SECURITY TRAINING COURSE

Thank you.

国内における制御システムの実態

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グループリーダ
山田 秀和

国内における制御システムセキュリティの実態

2014年2月5日
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
山田　秀和

目次

Ⅰ. JPCERT/CC2013年活動状況

Ⅰ.JPCERT/CC 2013年活動状況

■ 報告件数

5件

報告件数は、ご連絡頂きました件数であり
実際の対応件数とは異なります

Ⅰ.JPCERT/CC 2013年活動状況

- 実際の事例

  —インターネットに直接接続された制御システムや機器に関してのユーザ通知、対応

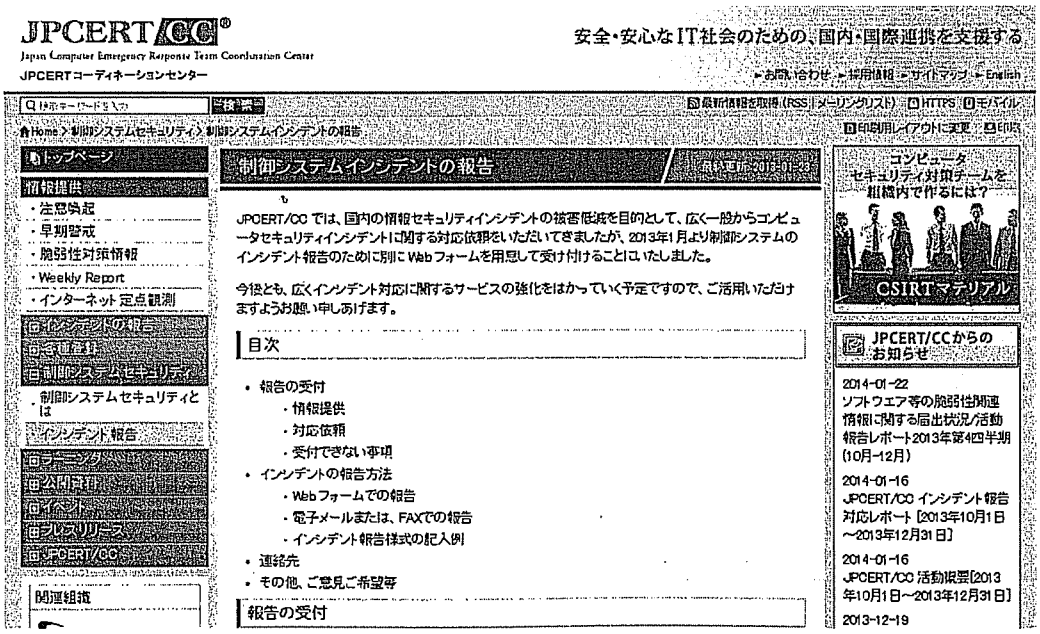
- 報告以外の事例

  —スキャン
  —踏み台

  など

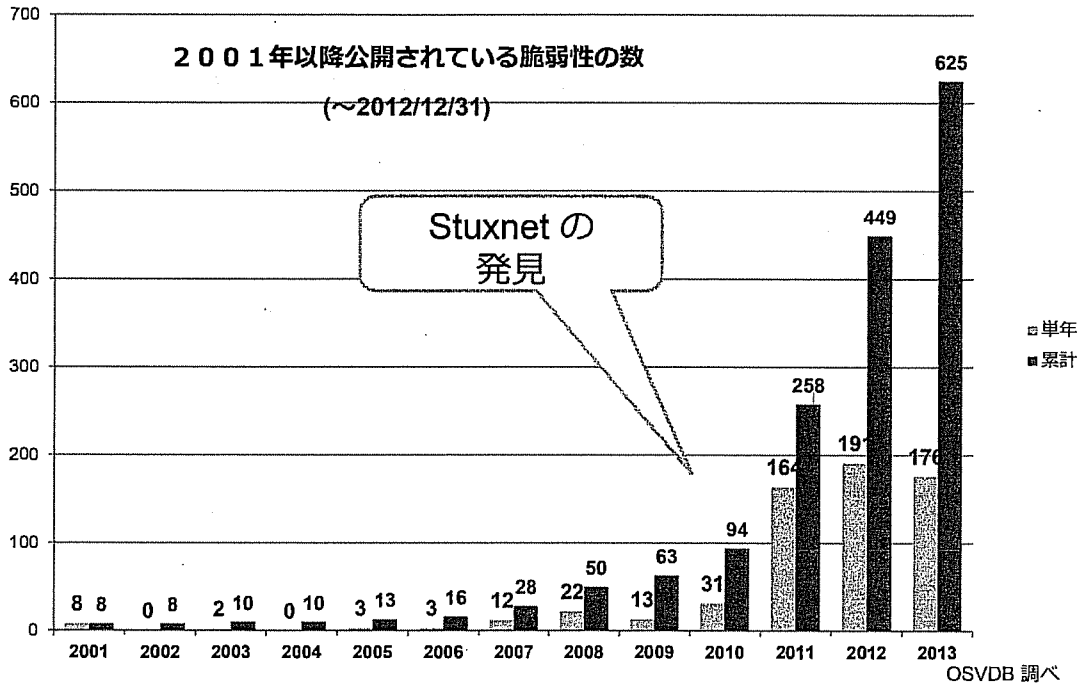
Ⅰ.JPCERT/CC 2013年活動状況

- 昨年のカンファレンスでも紹介させていただきましたが制御システムのインシデント受付は、Webサイトでも行っております（情報系も通常通り）



参考.2013年公表された脆弱性~公開情報を元に

制御システム関連製品の脆弱性



OSVDB 調べ

Ⅱ.JPCERT/CC調査結果（国内アセットオーナ）

Ⅱ.JPCERT/CC調査結果（国内アセットオーナー）

- インシデント（マルウエア感染数）

詳しくは
プレゼンにて
ご説明いたします

- 原因

詳しくは
プレゼンにて
ご説明いたします

Ⅱ.JPCERT/CC調査結果（国内アセットオーナー）

- セキュリティ情報の入手

詳しくは
プレゼンにて
ご説明いたします

- セキュリティ関連サポート

詳しくは
プレゼンにて
ご説明いたします

Ⅱ.JPCERT/CC調査結果（国内アセットオーナー）

- セキュリティリスクに関する評価

詳しくは
プレゼンにて
ご説明いたします

- 制御ネットワーク内でのセキュリティインシデント発生に関する意識

詳しくは
プレゼンにて
ご説明いたします

Ⅱ.JPCERT/CC調査結果（国内アセットオーナー）

- セキュリティインシデント発生時の相談先

詳しくは
プレゼンにて
ご説明いたします

- セキュリティインシデント発生に備えた体制

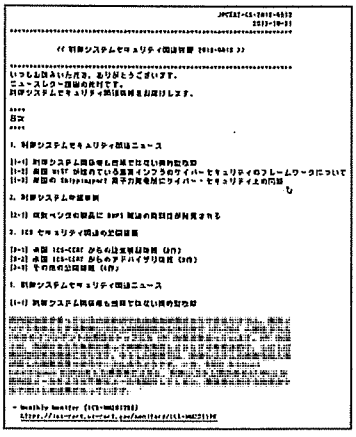
詳しくは
プレゼンにて
ご説明いたします

Ⅲ.情報共有

Ⅲ.情報共有

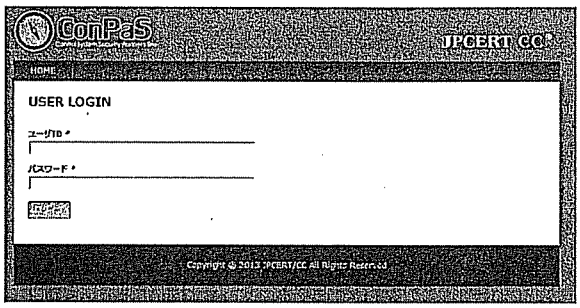
ニュースレター

月に一回発行



CONPAS

3月下旬にリニューアルします



勉強会

- アセットオーナー
- セキュリティ関連ベンダ・研究者

Ⅳ.まとめ

Ⅳ.まとめ

- セキュリティインシデントが起きた場合、責任を取るのはアセットオーナーの皆様です
- 現場の環境を知っている方を中心として、現状の把握をし、セキュリティインシデントが起こらないよう、起きた場合でも迅速に対応できるよう、情報収集、体制の確認、セキュリティの対策について考えてみましょう
- どうしたら良いのかわからない場合は、セキュリティベンダの方のサポートを受けることも一つの選択肢です
- 制御システムの仕組みを一番理解しているベンダ、エンジニアリング会社の方ともしっかりと話し合った上でセキュリティ対策を進めていきましょう

お問合せ、インシデント対応のご依頼は

JPCERT CC®
JPCERTコーディネーションセンター

安全・安心なIT社会のための、国内・国際連携を支援する
お問い合わせ サイトマップ English

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
- Email：icsr@jpcert.or.jp
- https://www.jpcert.or.jp/

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

インシデント報告
- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

JPCERT CC®
JPCERTコーディネーションセンター

安全・安心なIT社会のための、国内・国際連携を支援する
お問い合わせ サイトマップ English

ご静聴ありがとうございました