「2011年度重要インフラの共通脅威分析に関する調査」の結果について

2012年3月15日

内閣官房情報セキュリティセンター（NISC）

1.　2011年度の分析テーマと進め方 （1）

2011年度分析テーマ：「重要システムの堅ろう性について」

堅ろう性分析4つの視点　：分析の視点の明確化

システムをサイバー攻撃から守り、サービスを安定的に提供できることとし、以下のようなシステムを「堅ろう性が高い」とみなす。

① サイバー攻撃を受けにくいシステム

② サイバー攻撃を受けてもサービスを停止させないシステム

③ サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステム

④ サイバー攻撃によりサービスが停止しても早期に復旧できるシステム

（平成22年度内閣官房情報セキュリティセンター委託調査 「サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化に関する調査」 報告書　より）

1.　2011年度の分析テーマと進め方 （2）

■他分野の攻撃事例や最新の攻撃手法が自分野のシステムに潜在的にどのような影響をもたらすのか、気づきを与えるとともに、潜在的なリスクに対する想定される対策を示す。
　⇒　他分野の攻撃事例から自分野のシステムに潜むリスクについて気づきを与える。
■次年度以降の重要インフラ分野の施策に反映する。

文献調査　アンケート調査　ヒアリング調査　海外調査

Step 1	典型的攻撃事例の抽出	■最近の主要な攻撃事例を収集 ■収集された攻撃事例の中から要件に合致する典型的攻撃事例を抽出
Step 2	障害要因等の検討	■抽出された典型的攻撃事例について、障害要因・被害拡大要因を検討 ■障害要因・被害拡大要因は類型化12の視点から整理
Step 3	重要システムの類型化	■典型的攻撃事例の障害要因・被害拡大要因より、それに該当する重要システムを拾い上げる ■選択された重要システムを類型化のグループとする
Step 4	堅ろう性向上策の検討	■重要システムの類型毎に想定される具体的な堅ろう性向上策案について、実施可能性、有効性等の観点から検討を行う。

2.　典型的攻撃事例の抽出　＜Step1＞

■最近の主要な攻撃事例の中から、分析対象とする3要件(1)～(3)に該当する事例を抽出した。

典型的攻撃事例の要件定義

（1） 高度なスキルと確固たる動機を有す者による特定企業・組織を標的とした攻撃
（2） 汎用のNWに限らず、専用NWに接続された機器を標的とする攻撃手法
（3） セキュリティ上の脆弱性を悪用し、潜伏や拡散する手法を備えて被害を拡大させる攻撃手法

	略称	発生年月	業種（国）	概要
A	豪 下水処理場 不正アクセス	2000年 3月	水道 （オーストラリア）	クイーンズランド州マルーチー(Maroochy)市の上下水処理場において、元請負業者の技術者が、汚水処理管理システムをハッキングした。元請負業者の技術者との契約を切った後も当該システムのリモートアクセス用ID・パスワードを変更していなかった。元請負業者の技術者は正社員雇用の依頼を断られたことを逆恨みし、不正なリモートログインを続け、ポンプ場の下水処理システムを誤動作させ、上水処理システムのバルブを不正に閉じる等の操作をおこなった。
B	Operation Aurora	2009年 11月	各種 （米国）	2010年にGoogleが被害を公表することで明らかになった、Operation Auroraとは、IEの未知の脆弱性を利用した一連の攻撃であり、Google以外にも米国企業を中心に多くの企業が被害を受けたとされる。この攻撃により、中国反体制派に関する個人情報等が窃取されたとされる。
C	ソニー 不正アクセス	2011年 4月	家電 （日本・米国等）	海外ハッカーが公開したPS3のハッキングコードの公開差し止め訴訟が契機となり、これに反発したハッカー集団がソニー子会社のSCE及びSOEのサイトに不正侵入した。具体的には、攻撃者はアプリケーションサーバーに存在していた既知の脆弱性を利用して不正プログラムを埋め込み、外部からの侵入経路を確保。その後、データベースに不正アクセスすることで、個人情報を窃取したもの。
D	米原発 ワーム感染	2003年 8月	電力 （米国）	オハイオ州の原子力発電所でMicrosoft社のSQLサーバを狙ったSlammerワームに感染した。発電所のコンサルタント会社がSlammerワームに感染した端末にてリモートアクセスをし、ワームを蔓延させてしまった。
E	Stuxnet	2010年 8月	電力 （イラン）	Windowsの脆弱性を利用したワームStuxnetを入れ込んだUSBストレージを、不正に原子力発電所内に持ち込み、SCADA（Supervisory Control and Data Acquisition）システムとネットワーク上接続されているPCに接続してしまったことから感染してしまった。さらに感染後、Windows上で動作する独シーメンス社製ソフトウェアの脆弱性を利用してプラントを制御するPLC（プログラマブルロジックコントローラ）に悪質なコードを書き込んだ。

3．1　類型化の視点

■重要システムの堅ろう化に関するリスクと対策を考える場合、重要システムの特性に着目する必要がある。

■重要システムの内、最も特殊な形態と考えられる制御システムの特性に着目したうえで、その特徴（視点）として一般的なものを類型化の12の視点とする。

※類型化の視点の選定に当たっては、NIST, “Gude to Industrial Control System (ICS) Security” (SP800-82)及びSEMA(Swedish Emergency Management Agency),「重要社会インフラのための プロセス制御システム（PCS）の セキュリティ強化ガイド（JPCERT/CC訳）」を参考としたが、評価については独自に策定したものである。

視点	パフォーマンス（リアルタイム性）	可用性（高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
評価	情報セキュリティ対策よりも、リアルタイム性、応答時間を重視するシステムもしくは遅延が認められないシステムか否か。 1: セキュリティよりもパフォーマンス・リアルタイム性を重視 2: 可能であればセキュリティも考慮する 3: セキュリティを重視	情報セキュリティ対策よりも高可用性を重視するか否か。 1: セキュリティを重視 2: 高可用性を重視	情報セキュリティ対策よりも安全性を重視するか否か。 1: 機密性・完全性を重視（情報セキュリティを重視） 2: 安全性を重視	情報セキュリティ対策として、情報自体の保護を重視するか、端末等の物理的な保護を重視するか。 1: 情報の保護を重視 2: 両方重視 3: 端末等の物理的保護を重視	情報セキュリティ対策の適用がシステムに悪影響を与えるかどうか事前確認が必要か否か。 1: 影響は軽微もしくは無い 2: 悪影響を与える可能性大	緊急時において、アクセス制御を重視するのか、誰でも操作できる（対話操作の即時性）が重視されるのか。 1: アクセス制御を重視 2: 対話操作の即時性を重視

視点	システム運用と変更管理（特殊なシステム）	リソースに関する制約	通信（独自通信プロトコル）	サポート（少数ベンダー）	サービス稼働期間（長期稼働）	物理的アクセス（遠隔・分散）
評価	標準的なOSを用いているか、特殊なOSを用いているか。 1: 標準OS 2: 混在 3: 特殊OS	情報セキュリティ対策を実装するのに十分なリソースがあるか否か。 1: リソースが十分 2: リソースが不十分	標準的な通信ネットワークを用いているか、独自・特殊な通信ネットワークを用いているか。 1: 標準 2: 混在 3: 独自・特殊	サポート窓口となるベンダーの数。 1: 多数 2: 少数（1～2社）	システム稼働期間が短期か長期か。 1: 短期（3～5年） 2: 中間（6年～14年） 3: 長期（15年～）	システムが管理者の近隣に設置されているのか、遠隔地に設置されていたり分散しているのか。 1: 近隣 2: 中間 3: 遠隔（分散）

3．2　典型的攻撃事例の障害要因等整理　＜Step2＞　（1）

■典型的攻撃事例それぞれについて、類型化の12の視点と（その他）の計13の視点に基づき、抽出事例の詳細分析を通じて障害要因等を検討　　※下線を引いた要因は特徴的な障害要因等を示す

豪下水処理場不正アクセス

パフォーマンス（リアルタイム性）	可用性（高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
ー	障害発生後もシステムを停止して調査していない。	ー	ー	侵入検知システムが整備されていなかった。	対話操作の即時性を悪用。
システム運用と変更管理（特殊なシステム）	**リソースに関する制約**	**通信（独自通信プロトコル）**	**サポート（少数ベンダー）**	**サービス稼働期間（長期稼働）**	**物理的アクセス（遠隔・隔離）**
制御システムに使われる機器を盗難し不正侵入に用いた。	ー	制御用の無線システムを用いた侵入。	ー	ー	遠隔にある制御システムへの無線システムを用いた直接的な侵入。
その他					
削除されなかった退職者のアカウントを利用した不正アクセス。	機器の盗難防止対策が不十分だった。	ー	ー	ー	ー

Operation Aurora

パフォーマンス（リアルタイム性）	可用性（高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
ー	ー	ー	ー	ー	ー
システム運用と変更管理（特殊なシステム）	**リソースに関する制約**	**通信（独自通信プロトコル）**	**サポート（少数ベンダー）**	**サービス稼働期間（長期稼働）**	**物理的アクセス（遠隔・隔離）**
社内用アプリケーション（ソースコード管理システム）のセキュリティ対策が不十分。	ー	ー	よく用いられる社内用アプリケーションのベンダーが少ないため、同種攻撃が他企業に対しても行われやすい。	ー	ー
その他					
メッセージの信ぴょう性をユーザーが正しく判断することは困難。	ゼロデイ脆弱性を防御することは困難。	ー	ー	ー	ー

3．2　典型的攻撃事例の障害要因等整理　＜Step2＞　（2）

ソニー不正アクセス	パフォーマンス（リアルタイム性）	可用性（高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
	ー	稼働中のアプリケーションの脆弱性を修正できなかった。	ー	ー	ー	ー
	システム運用と変更管理（特殊なシステム）	リソースに関する制約	通信（独自通信プロトコル）	サポート（少数ベンダー）	サービス稼働期間（長期稼働）	物理的アクセス（遠隔・隔離）
	ー	ー	ー	運営子会社に関する管理が不十分だった（個人情報保護法違反）。	ー	ー
	その他					
	ハッカーコミュニティとのコミュニケーションの取り方を間違えた。	システムを稼働する際のセキュリティ検査が不十分だった。	ログの削除を防ぐような仕組みを導入していなかった。	暗号鍵を容易にアクセスできる場所で管理していた場合、クレジットカード情報も復号される可能性。	事態発覚から主務省・顧客への報告までの期間が長すぎるとの批判を受けた。	ー

米原発ワーム感染	パフォーマンス（リアルタイム性）	可用性（高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
	ー	可用性を重視したため、既知の脆弱性に対する対策が不十分だった。	セキュリティパッチ適用による障害発生を懸念した可能性。	ー	発電所システムにパッチを当てたうえでテストを行う事が困難な要因があった可能性。	ー
	システム運用と変更管理（特殊なシステム）	リソースに関する制約	通信（独自通信プロトコル）	サポート（少数ベンダー）	サービス稼働期間（長期稼働）	物理的アクセス（遠隔・隔離）
	汎用的なシステムは一部で利用されており、ウイルス等の影響を受けた。	発電所システムにパッチを当てたうえでテストを行う事が困難な要因があった可能性。	メンテナンス用リモートアクセス回線からの侵入。 ネットワーク能力の飽和に関する考慮不足。 機器間の相互依存性に対する考慮不足。	特定ベンダー等への依存が強すぎることにより、不必要な権限を与えていた可能性。 外注先のPC等の安全性に関する委託先の監督が不十分であった。	ー	遠隔にあるが故のメンテナンス方法を残したことが侵入に繋がった。
	その他					
	ー	ー	ー	ー	ー	ー

3．2　典型的攻撃事例の障害要因等整理　＜Step2＞（3）

Stuxnet	パフォーマンス（リアルタイム性）	可用性 （高可用性）	リスクマネジメント（安全性優先）	セキュリティアーキテクチャ（物理的保護）	セキュリティソリューション（対策の制約）	対話操作の即時性（操作への応答性）
	ー	可用性を重視したため、既知の脆弱性に対する対策が不十分だった。	パスワードをハードコーディングするという通常システムでは考えられないセキュリティ設計。	物理的な保護に依拠するシステムにもかかわらず、USB等の裏口の管理が不十分だった。	USBドライブの利用を限定するようなセキュリティソリューションの利用を怠った。 IDS等の侵入検知ソリューションを十分に活用できなかった。	ー
	システム運用と変更管理（特殊なシステム）	リソースに関する制約	通信 （独自通信プロトコル）	サポート （少数ベンダー）	サービス 稼働期間（長期稼働）	物理的アクセス（遠隔・隔離）
	特殊なシステムでも十分な調査を行えば、脆弱性を発見可能。 オープンシステムの利用による既知の脆弱性が弱点となった。	ー	ー	重要なシステムは一社が提供していた。	ー	ネットワークが物理的に隔離されていたシステムであっても、セキュリティ対策上見落とされていた侵入路が利用された。
	その他					
	当該技術者の特定と、誘因（USBを受け取りたくなる）の把握を許した。	ー	ー	ー	ー	ー

4．1　類型化の手法

■「重要システムの分析」及び「障害要因等の検討」の結果を踏まえ、以下の手順で「重要システムの類型化」を行う。

①攻撃事例の要因（3.2典型的攻撃事例の障害要因等整理）より、**特徴的な障害要因等が属する視点**（3.1類型化の視点）を抽出する。
※今回の分析においては、特徴的な障害要因等以外の障害要因については分析の対象外とした。
②分析対象となる重要システムについて、①で抽出した特徴的な障害要因等が属する視点から、**その該非についてそれぞれ判断を行う。**
③①で抽出した全ての特徴的な障害要因等が属する視点に関して、②で実施した該非判定が**全て適合する場合、「特徴的な障害要因等に該当する可能性があるシステム」と判断する。**

①検討対象の攻撃事例の要因の中で、**特徴的な障害要因が属する視点**を抽出（本例では赤枠の3要因）

攻撃事例の障害要因等調査

豪下水処理場不正アクセス	パフォーマンス（リアルタイム性）	…	システム運用と変更管理（特殊なシステム）	リソースに関する制約	通信（独自通信プロトコル）	…	サービス稼働期間（長期稼働）	物理的アクセス（遠隔・隔離）
	ー	…	制御システムに使われる機器を盗難し不正侵入に用いた。	ー	制御用の無線システムを用いた侵入。	…	ー	遠隔にある制御システムへの無線システムを用いた直接的な侵入。

重要システムの分析

システム	パフォーマンス	…	システム運用と変更管理	リソースに関する制約	通信	…	サービス稼働期間	物理的アクセス
Aシステム	2	…	2	2	2	…	3	3
Bシステム	1	…	2	2	3	…	3	1

②Aシステム＝該当
Bシステム＝該当

②Aシステム＝該当
Bシステム＝該当

②Aシステム＝該当
Bシステム＝非該当

③Aシステムは3要因全てが該当

③Bシステムは3要因中2要因のみ該当

4．2　重要システムの類型化（整理表）　＜Step3＞

■類型化の視点に基づき、全重要システムについてセキュリティに影響を与える特性を分析した。
※アンケート／ヒアリングの結果を反映したが、回答結果が必ずしも自分野の重要システムの特性を代表しているとは言えず、また視点によっては重視する側を択一回答するのが難しい場合もあったことから、特性の分析結果は「一つの代表例」として扱う。
※以後の分析手法に供する例として重要システムの中から10種を任意に選択したうえで、システム名をふせて以下に例示する。

システム	パフォーマンス	可用性	リスクマネジメント	セキュリティアーキテクチャ	セキュリティソリューション	対話操作の即時性	システム運用と変更管理	リソースに関する制約	通信	サポート	サービス稼働期間	物理的アクセス
Aシステム	2	2	2	3	2	2	2	2	2	1	3	3
Bシステム	1	2	2	3	2	2	2	2	3	2	3	1
Cシステム	3	1	1	2	1	1	1	1	1	1	1	1
Dシステム	1	2	2	3	2	2	2	1	2	2	3	2
Eシステム	2	2	2	1	1	1	1	2	1	2	1	1
Fシステム	2	2	2	2	2	1	2	1	2	1	2	1
Gシステム	1	2	2	2	2	2	3	1	3	2	2	1
Hシステム	2	1	1	2	2	2	3	1	2	2	3	1
Iシステム	3	1	2	1	1	1	1	1	1	1	1	2
Jシステム	2	2	2	2	1	1	2	1	1	1	2	3

凡例

1: セキュリティよりもパフォーマンスを重視 2: 可能であればセキュリティも 3: セキュリティを重視	1: セキュリティを重視 2: 高可用性を重視	1: 機密性・完全性を重視 2: 安全性を重視	1: 情報の保護を重視 2: 両方重視 3: 端末等の物理的保護を重視	1: 影響は軽微もしくは無い 2: 悪影響を与える可能性大	1: アクセス制御を重視 2: 対話操作の即時性を重視	1: 標準OS 2: 混在 3: 特殊OS	1: リソースが十分 2: リソースが不十分	1: 標準 2: 混在 3: 独自・特殊	1: 多数 2: 少数（1～2社）	1: 短期（3～5年） 2: 中間（6年～14年） 3: 長期（15年～）	1: 近隣 2: 中間 3: 遠隔（分散）

システム	典型的攻撃事例				
	豪下水処理場不正アクセス	Operation Aurora	ソニー不正アクセス	米原発ワーム感染	Stuxnet
Aシステム	○		○		
Bシステム		○		○	○
Cシステム			○		
Dシステム	○	○		○	○
Eシステム					○
Fシステム			○		
Gシステム		○		○	
Hシステム		○		○	○
Iシステム			○		
Jシステム		○	○	○	

※本表において○が付されたものは、同種の攻撃リスクがあることを示しているが、対策の不備や脆弱性が存在することを意味するものではない。

5.　典型的攻撃事例と堅ろう性向上策の整理（1）　＜Step4＞

■堅ろう性向上策について、Step3の整理表（各典型的攻撃事例に対する各重要システムの潜在リスク）及び堅ろう性分析の4つの視点との関連付けを行った。

※以下の整理において、〇は特に関係があるものに付されたものであるため、空欄であっても関係が無いということを意味しているわけではない。

有効な対策項目			典型的攻撃事例※1					堅ろう性分析4つの視点※2			
No		具体策	A	B	C	D	E	①	②	③	④
A）物理的隔離による侵入の防御	物理的対策	外部記憶媒体・通信用コネクタのポートに蓋をする	〇				〇	〇	〇		
		入退出管理の厳格化	〇				〇	〇	〇		
		ネットワークや端末の分離	〇			〇	〇	〇	〇	〇	
	システム的対策	デバイスドライバを削除する	〇				〇	〇	〇		
		外部記憶媒体の挿入やネットワークへの接続を検出する	〇				〇	〇	〇		
B）論理的隔離による侵入の防御	境界防御	FWの多重化	〇		〇		〇	〇	〇	〇	
		DMZの多重化	〇		〇		〇	〇	〇	〇	
		検疫ネットワークの設置	〇		〇		〇	〇	〇	〇	
		ブロック化	〇		〇		〇	〇	〇	〇	〇
		アプリケーションゲートウェイの導入	〇	〇	〇		〇	〇	〇	〇	
	仮想化	サーバー等の仮想化	〇				〇	〇	〇	〇	〇
	秘匿による防御	VPN（IPSec等）の導入	〇		〇		〇	〇	〇		
		特殊なプロトコル・HW等を導入する	〇				〇	〇	〇	〇	
C）攻撃や侵入の検知能力の向上	入口対策	IDSの導入	〇	〇	〇		〇		〇	〇	
		高度な侵入検知技術の導入（振る舞い検知・ヒューリスティック）	〇	〇	〇		〇		〇	〇	
		フィルタリング技術の導入（ホワイトリスト・ブラックリスト）	〇	〇	〇		〇	〇	〇	〇	

※1：典型的攻撃事例に特に有効と考えられる対策に〇を付与したものであり、空欄となっている対策が不要であるということを意図したものではない。凡例は「2．典型的攻撃事例の抽出　＜Step1＞」を参照。
※2：凡例は「1．2011年度の分析テーマと進め方（1）」を参照。

5.　典型的攻撃事例と堅ろう性向上策の整理（2）　＜Step4＞

有効な対策項目			典型的攻撃事例※1					堅ろう性分析4つの視点※2			
No		具体策	A	B	C	D	E	①	②	③	④
C）攻撃や侵入の検知能力の向上	出口対策	DLP (Data Loss Prevention)　技術の導入	○	○	○		○			○	○
		出口認証	○	○	○		○		○	○	○
	組織的対策	監視体制の整備	○	○	○		○		○	○	
		ログの保存	○	○	○		○			○	○
	サーバーの堅ろう化	ハードニング	○	○	○		○	○	○	○	○
		OSにおける最小限のサービスの導入	○	○	○		○	○	○	○	
		改ざん検知	○	○	○		○		○	○	○
D）パッチマネジメント等の計画的な脆弱性対策の実施	運用的対策	ベンダーとパッチマネジメントを含む契約を締結			○	○	○	○	○		
		ベンダーとの定期的な協議の実施			○	○	○	○	○	○	○
		パッチマネジメントルールの策定			○	○	○	○	○		
	技術的対策	パッチ適用可否を判断するためのテスト環境の整備			○	○	○	○	○		
		予備系統を利用したパッチの安全な適用	○	○	○	○	○	○	○		
E）システムの2重化等の緊急障害回避策	物理的配置	遠隔地にデータをバックアップ	○	○		○	○		○	○	○
		遠隔地にバックアップシステムを設置	○	○		○	○		○	○	○
	技術的対策	情報システムの二重化（多重化）	○	○		○	○		○	○	○
		多様性の確保	○	○	○	○	○	○	○	○	○
		通信回線の多重化、冗長化	○	○		○	○		○	○	○
		物理的保護機能（インターロック）・フェイルセーフ	○	○		○	○		○	○	○

※1：典型的攻撃事例に特に有効と考えられる対策に○を付与したものであり、空欄となっている対策が不要であるということを意図したものではない。凡例は「2．典型的攻撃事例の抽出　＜Step1＞」を参照。
※2：凡例は「1．2011年度の分析テーマと進め方（1）」を参照。

5.　典型的攻撃事例と堅ろう性向上策の整理（3）　＜Step4＞

有効な対策項目			典型的攻撃事例※1					堅ろう性分析4つの視点※2			
No		具体策	A	B	C	D	E	①	②	③	④
F）ID・パスワード等の管理強化	生体認証	指紋・静脈・虹彩認証等の導入	○					○			
	シングルサインオン	シングルサインオンシステムの導入	○					○			
		人事情報システムとの連携	○					○			
	アクセス管理の厳格化	コマンド実行時にもID/PWを要求する	○					○			
		出口認証（再掲）	○	○	○		○	○			
		不要IDの削除	○					○			
		IDの使い回し禁止	○					○			
G）外注・グループ会社内のセキュリティポリシーの共有化	契約前	契約時にセキュリティ条項を課す	○		○	○		○	○	○	○
		セキュリティ教育の実施を求める	○		○	○		○	○	○	○
	契約後	対策実施状況の抜き打ち報告	○		○	○		○	○	○	○
		外注先等の定期的監査	○		○	○		○	○	○	○
H）経営層の関与も含めたITガバナンス体制の構築と開発計画等（EA等）の策定	マネジメント	責任者（CIO、CISO、情報セキュリティ委員会等）の設置			○			○	○	○	○
		リスクマネジメント			○			○	○	○	○
		事業継続マネジメント			○				○	○	○
	開発	開発マニュアルの整備			○			○	○	○	○
		システム重要性のランク付け			○			○	○	○	○
I）ベンダー等、社外組織との連携・協力体制の構築	ベンダーとの連携	ベンダーによるユーザ企業教育の実施	○			○		○	○	○	○
	業界内での連携	日常からの情報交換	○	○	○	○	○	○	○	○	○

※1：典型的攻撃事例に特に有効と考えられる対策に○を付与したものであり、空欄となっている対策が不要であるということを意図したものではない。凡例は「2．典型的攻撃事例の抽出　＜Step1＞」を参照。
※2：凡例は「1．2011年度の分析テーマと進め方（1）」を参照。

5.　典型的攻撃事例と堅ろう性向上策の整理（4）　＜Step4＞

有効な対策項目			典型的攻撃事例※1					堅ろう性分析4つの視点※2			
No		具体策	A	B	C	D	E	①	②	③	④
J）長期にわたるシステムライフサイクルを考慮したセキュリティ確保	更新計画策定	システム更新計画の策定	○			○	○	○	○		
		システム更新基準（故障率、保守終了等）の策定	○			○	○	○	○		
	ベンダーとの協力	情報提供（製造完了、保守終了等）の依頼	○			○	○	○	○		
		保守用部品の確保	○			○	○	○	○		
K）セキュリティに関するPDCAの実施（セキュリティ監査等の実施を含む）	ー	自主検査・監査	○	○	○	○	○	○	○	○	○
		第三者監査の実施	○	○	○	○	○	○	○	○	○
		外注先等の定期的監査（再掲）	○		○	○		○	○	○	○
		訓練・演習の実施	○	○	○	○	○		○	○	○
L）その他	インシデント対応	インシデント対応人材の育成	○	○	○	○	○		○	○	○
		インシデント対応手順の策定	○	○	○	○	○		○	○	○
	ー	データの暗号化		○	○					○	
		機器の盗難防止	○					○			
		ネットワーク構成等に関わる情報を秘匿する	○				○	○	○		

※1：典型的攻撃事例に特に有効と考えられる対策に○を付与したものであり、空欄となっている対策が不要であるということを意図したものではない。凡例は「2．典型的攻撃事例の抽出　＜Step1＞」を参照。
※2：凡例は「1．2011年度の分析テーマと進め方（1）」を参照。

6.　海外の重要インフラシステムの堅ろう性向上策についての調査結果

■重要インフラ（主に制御系システム）におけるStuxnet後の対応状況の例について、ヒアリング調査等によりまとめた。

	欧州	米国
重要インフラ事業者	・重要インフラ事業者、政府間における情報共有体制としてEuro-SCSIEが立ち上がっている。 ・ベンダーに対するセキュリティ要件等を策定する活動である、WIB(International Instrument Users' Association）がドイツとオランダの事業者が中心となって設立された。	・電力分野ではNERC、公共交通分野APTAなどの業界団体がセキュリティ基準を策定もしくは策定中。APTAの基準策定にはDHSも関与。
ベンダー	・Stuxnetを踏まえ、中小規模から大規模なベンダーまで対策を進めているが、中小ベンダーの方が機動性があり、対策済み製品をリリースし始めている（ドイツの事例）。	・国立研究所Idaho National Laboratory (INL) の施設を利用した製品の検証。
政府	・重要インフラ事業者、政府間における情報共有体制としてEuro-SCSIEが立ち上がっている（再掲）。 ・ENISAにおいてSCADAセキュリティに関する産官学による検討を行い報告書を発行している。 ・欧州サイバー演習の実施	・DHSの主催で官民が参加する Industrial Control System Joint Working Groupを開催している。 ・Idaho National Laboratory (INL) の施設を利用した製品の検証（再掲）。

7.　重要システムの堅ろう性についての考察と課題

課題	課題内容	今後求められる対応
1.物理的隔離のみに依拠した情報セキュリティ確保の限界	■業務上の必要性から、可搬型媒体の利用を禁止できない場合や、外部ネットワークからの完全な隔離が出来ない場合がある。 ■モバイル端末等の普及や社会的要請（重要システム・サービスの稼働状況等の公表等）に対応するため、従来は外部から隔離されていた重要システムを情報共有等の目的で外部システムに連接する必要が出てきている。	■今後の技術トレンドや社会的要請を想定すると、物理的隔離に依拠したセキュリティ確保はますます困難になっていくことが想定される。 ■物理的隔離が保障されない事を前提として、5.に掲げた対策を組み合わせるなどによる補完的対策を講じることを検討するべきである。
2.重要システムにおけるパッチマネジメント	■重要システムに対してセキュリティパッチやアップデートを行う事は以下のような理由から困難を伴う場合がある。 • システムを簡単に停止できない • パッチ等の適用が本来機能に与える影響を事前に検証することが困難 • システムリソース（処理速度や記憶容量等）の制約からアップデート等が困難 ■最近はインターネット経由のアップデートが主流のため、物理的に隔離されたシステムの場合アップデートを行うためには、外部ネットワークにつながなければならないなどの矛盾が生じている。	■サービス中断の緊急回避策として多重化されているシステムにおいては、待機側のシステムをテスト環境として利用し、事前検証して影響を確認したうえでアップデートを順次実施することが望ましい。 ■コスト面での制約や、その他の事由によって多重化システムを利用した事前検証が困難なシステムにおいては、今後の仮想化技術等の進展による新たなテスト環境の整備も期待される。 ■運用する重要システムに関する脆弱性対策について、どういう管理の下で、どういう手段で実施すべきか関係者による協議が必要。
3.重要システムにおける競争入札と情報セキュリティ	■一般競争入札等により、情報セキュリティも含む仕様が公開されると脆弱性を類推しやすくなることから、攻撃のハードルが下がる可能性がある。特にWTO政府調達協定の対象となる重要インフラ事業者は、対象案件について入札説明書を公開するなどが求められている。 ■将来的な脅威について予測することはできないため、セキュリティ仕様を調達時に明確化することができない。そのため競争入札においては、セキュリティ面で余裕のあるシステムを調達することが困難であり、特に長期稼働するシステムにおいては大きな問題となりうる。	■競争入札においても、情報セキュリティに係る部分については、可能な範囲で開示を制限するなどの工夫が必要である。WTO政府調達の対象であっても、安全保障を理由とし必要な措置をとることを防げないとされていることから、同条項の積極的な活用も念頭においての検討。 ■将来的な脅威を予想することが出来なくとも、情報セキュリティの観点から、どの程度リソースに余裕を持たせると長期稼働に耐えるのか等についての検討。
4.未然防止型のみの情報セキュリティ対策の限界	■未然防止型の情報セキュリティ対策に限界が見えてきている。 • 攻撃者の技術・能力の向上 • 情報システムの複雑化	■侵入が避けられないことを前提に、被害の発生・拡大防止や早期復旧に効果のある対策を講ずる必要がある。また事業継続マネジメントとの連携が重要となる。 ■人材の育成、特に事業継続やインシデント対応などの危機対応型の人材を育成していく必要がある。 ■情報共有体制の強化による対応能力の向上。 • 重要インフラ事業者だけでなく、重要インフラを支えるベンダーやシステム子会社の参加 • インシデント対応の組織体制の構築
5.重要システムをとりまく新たな脅威とリスク	■業務の変化 • 業務の複雑化に伴う情報システムの複雑化。特に情報系、業務系の繋ぎの部分など。 • 事業継続の観点から、いわゆる重要システムに加え、事務系システムの重要性が再認識されている。 ■技術の変化 • モバイル機器、特にスマートフォンの利用拡大。重要インフラにおいても、保守用途等で普及の兆し。 • 情報系システムのリアルタイムシステム化の進展、制御システムと一般システムの境界の曖昧化。 ■社会の変化 • 製品の汎用化、海外進出の活発化による技術的知識の拡散。	■官民連携によって重要インフラをとりまく新たな脅威とリスクの動向を継続的に監視し、情報共有と意見交換を行う仕組みが必要

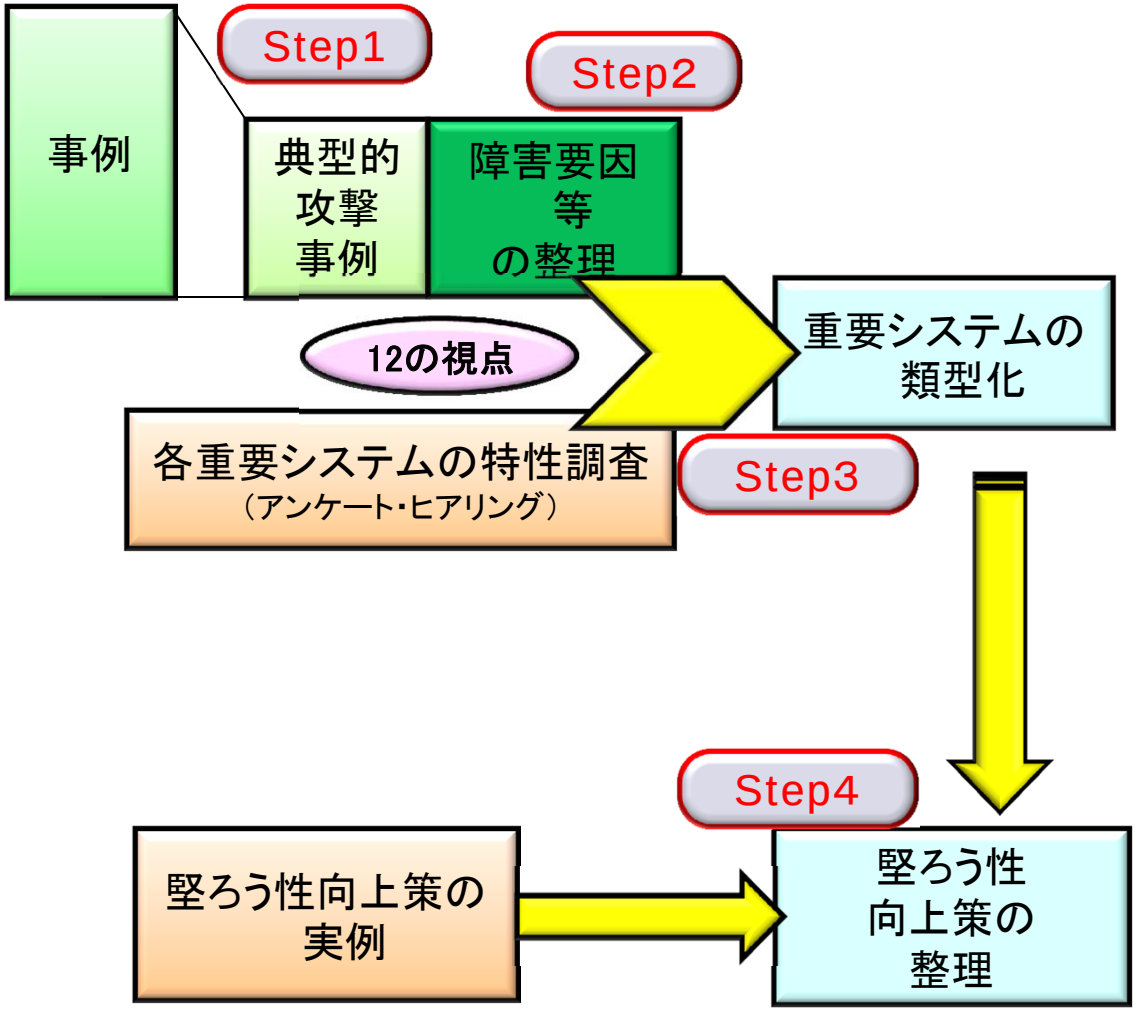
8.　分析結果の活用方法について（1）

■過去の典型的攻撃事例それぞれについて自分野の重要システムに係る潜在リスクを自己評価したうえで、堅ろう性向上に向けての具体策を自己点検する新しい手法を提示する。

○過去の攻撃事例を本分析で定めた3つの視点に沿って分析し、典型的攻撃事例として5つの事例を抽出したうえで、それぞれの事例の障害要因を「類型化の12の視点」で整理。（Step1～Step2）

○自分野の各重要システムの特性を、同じ「類型化の12の視点」に沿って整理し、先出の典型的攻撃事例の整理結果と重ね合わせることによって、各システムに潜む同様の攻撃に対するリスクを自己評価。（Step3）

○各分野で導入されている具体策を挙げ、それらの典型的攻撃事例への有効性を整理したことで、自社の導入対策の堅ろう性について自己点検。（Step4）



8.　分析結果の活用方法について　（2）

1 将来**新たな攻撃事例が発生した際**には、本分析にて提示した**「類型化の12の視点」**に沿って整理する手法によって、他分野で発生した攻撃事例と同様の手口によって障害が生じうる潜在リスクを自己評価することができる。（Step2～Step3）

2 ある攻撃事例に対して、その**潜在リスクを自己評価すべき分析対象システムが生じた場合**にも、本分析にて提示した手法を適用することができる。（重要システム以外のシステムでも適用可）