リスクアセスメントサービス

2025年1月
技術研究組合制御システムセキュリティセンター

CSSCのリスクアセスメントについて

技術研究組合制御システムセキュリティセンタ（CSSC）は、相当数の制御システム等を対象にリスクアセスメントを実施してまいりました。

その知見を活用し、制御システムのオーナーやベンダの皆様にリスクアセスメントサービスをご提供する所存です。

CSSCのリスクアセスメントの特徴は、CSSCが有している独自の攻撃シナリオとチェックリストをもとに事業継続上の脅威を発現しうる攻撃シナリオとチェックリストにより、攻撃シナリオ毎の対策の実装状況を評価し、対策計画を策定することにあります。

本資料をご参照頂き、CSSCのリスクアセスメントサービスの活用をご検討下さいますようお願い申し上げます。

技術研究組合制御システムセキュリティセンター
事務局長　村瀬一郎

リスクアセスメントとは

リスク分析：
リスクの特質を理解し，リスクレベルを決定するプロセス（(ISO 31000）

リスクを発見し、リスクの大きさを判断し、対策の方向性および対策の実装の是非を決定するプロセス（本講義においては、リスクアセスメントも同義）

リスクアセスメントは、製品の企画開発・設計・製造の各段階から、製品が流通に置かれ、使用され、廃棄されるまでのライフサイクルにおけるプロセス全般において実施されることが重要です。製造業者等や製品の安全性に係わる組織等は、より安全なものづくりのために出荷前までの各工程の要所で適切なリスク評価を実現するのはもちろんのこと、流通後も想定できなかった使用環境による不具合の発生はないか、科学技術の進歩により新たに解明されたリスクは存在しないか等、市場やユーザーの実態と最先端の科学的知見の動向を監視し続け、評価の見直しを適宜実施することにより、社会の期待に応えることが求められます。

経済産業省　リスクアセスメント・ハンドブック

リスクアセスメント手法の種類と特徴

リスクアセスメント手法	説明
ベースラインアプローチ	既存の標準や基準をもとに、予め一定の確保すべきセキュリティ水準を設定し、対象となるシステムの到達度合等をチェックする。
非形式的アプローチ	組織や担当者の経験や判断によってリスクを評価する。
詳細リスクアセスメント	詳細なリスクアセスメントを行うため、システムに対し、「重要度」、「脅威」、「ぜい弱性」を識別し、評価する。
組み合わせアプローチ	複数のアプローチを併用し、作業の効率化、分析精度の向上を図る。
シナリオベースアプローチ	事業継続上の脅威を発現しうるサイバー攻撃シナリオを作成し、それらシナリオに対する対策チェックリストにより、個々のシナリオの発現可能性を評価する。

CSSC推奨

「電力制御システムセキュリティガイドライン」にCSSCが加筆

リスクアセスメントのポイント

- リスクアセスメントは、技術や環境変化に伴い適宜実施することが重要であり、1回限りでは不十分
- ベースラインアプローチ、CSMS等においては、ある時点における評価を行うが継続性が重要
- 事業継続上の脅威を明確化することにより、その発現のための攻撃シナリオを作成可能
- 資産の網羅性を担保しても、脆弱性の網羅性を担保することは不可能
- 脆弱性の網羅性を担保するには、システム構成や稼働環境、一般的な脆弱性情報および攻撃情報等を勘案した、技術面と運用面に係る独自の視点（チェックリスト）を設定

CSSCは、シナリオベースを繰り返し実施することを推奨

CSSCのシナリオベースアセスメントの特徴

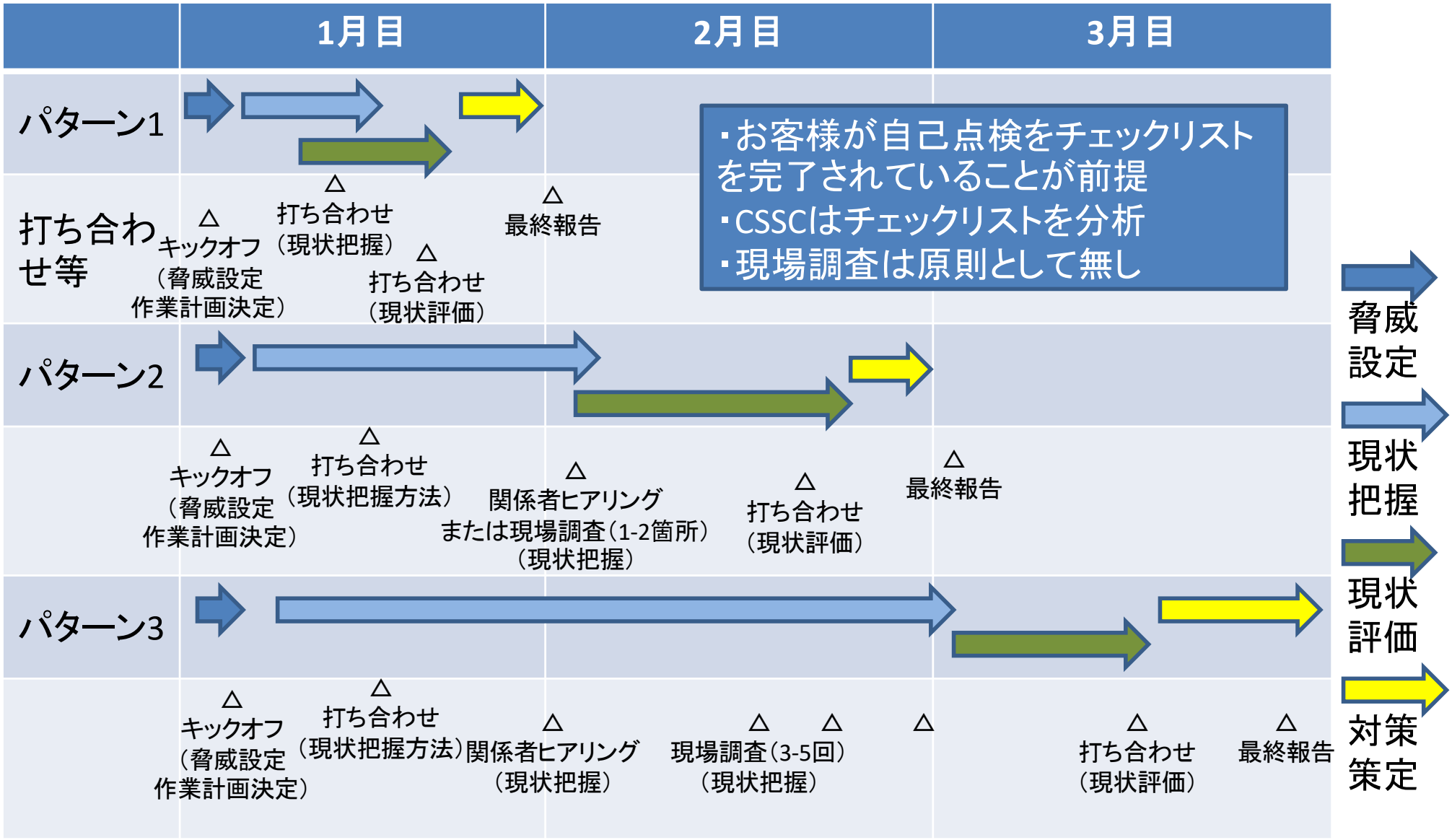
1. 制御システムの特徴を踏まえた攻撃シナリオ
   過去のサイバー攻撃や事故等CSSCの有する知見をもとに作成
2. 年度毎に対策がなされている攻撃を明確化
   経営幹部に年度毎の進展を視覚化し報告可能
3. 対象とする制御システムは各分野の制御システムと施設制御システム
   施設制御システム（電源系、空調系統）は、全ての制御システムにとって依拠するシステム

※なお、本シナリオベースアセスメントは経済産業省の「情報セキュリティ監査基準」に準拠しております。

リスクアセスメントの全体像

1	2	3	4
事業継続上の脅威の設定	チェックリストによる現状把握	攻撃シナリオ毎の現状評価	対策計画の策定
対象となる制御システムの異常に伴う事業継続上の脅威を設定	CSSCが有する制御システムへの典型的な攻撃シナリオをもとに作成したチェックリストにより、現状を把握	現状把握結果をもとに、攻撃シナリオ毎の現状を評価	対策が必要な事項に関して、対策の是非を判断

作業イメージ

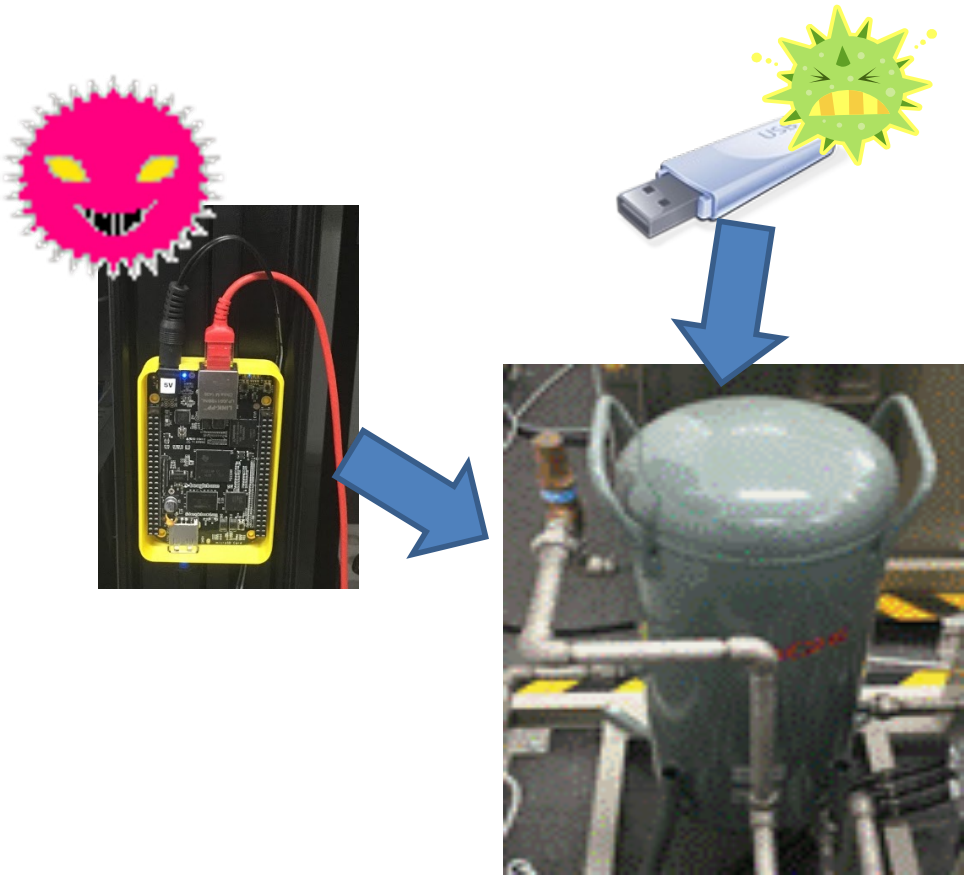

1月目
2月目
3月目
パターン1
打ち合わせ等
パターン2
パターン3
・お客様が自己点検をチェックリストを完了されていることが前提
・CSSCはチェックリストを分析
・現場調査は原則として無し
△キックオフ（脅威設定 作業計画決定）
△打ち合わせ（現状把握）
△打ち合わせ（現状評価）
△最終報告
△キックオフ（脅威設定 作業計画決定）
△打ち合わせ（現状把握方法）
△関係者ヒアリング または現場調査（1-2箇所）（現状把握）
△打ち合わせ（現状評価）
△最終報告
△キックオフ（脅威設定 作業計画決定）
△打ち合わせ（現状把握方法）
△関係者ヒアリング（現状把握）
△現場調査（3-5回）（現状把握）
△打ち合わせ（現状評価）
△最終報告
脅威設定
現状把握
現状評価
対策策定

作業イメージの説明

	対象システム数	現場把握の方法	現場調査	打ち合わせ回数
パターン1	原則1システム	原則ヒアリングのみ、またはお客様記入済みのチェックリストの分析	なし	3-4回程度
パターン2	原則2-3システム程度	CSSC所有のチェックリストにより、ヒアリングと現場調査により分析	あり（1-2カ所程度）	5-6回程度
パターン3	4システム以上	CSSC所有のチェックリストにより、ヒアリングと現場調査により分析	あり（3-4ヶ所以上）	7-8回程度

・どのパターンでも、シナリオベースのリスクアセスメント実施
・現場調査の対象は、サーバルーム、監視室、フィールド機器の設置場所に加え、電力、水の受給装置等

制御システムへのサイバー攻撃シナリオ（一部）



制御システムへのサイバー攻撃シナリオ(1)

外部媒体や持込PCからのマルウェア感染

- USBメモリ等の外部媒体がHMI端末やエンジニアリング端末に装着されることによりマルウェアが感染する
- 保守用持込PCからマルウェアが感染する

具体例	
	• 外部記憶媒体（USBメモリ、USB接続外付けHDD、スマートフォン等）にマルウェア感染 • USB Type-CやHDMIを介してマルウェア感染

対策例	・隔離環境におけるウィルスチェック ・USBポートの管理 ・USBメモリの管理 ・ホワイトリスト導入　他

制御システムへのサイバー攻撃シナリオ(2)

不正な攻撃用端末接続による中間者攻撃

- 攻撃者は攻撃対象に到達するために、物理セキュリティを突破し空きポートに攻撃用端末を接続することにより、中間者攻撃を実施

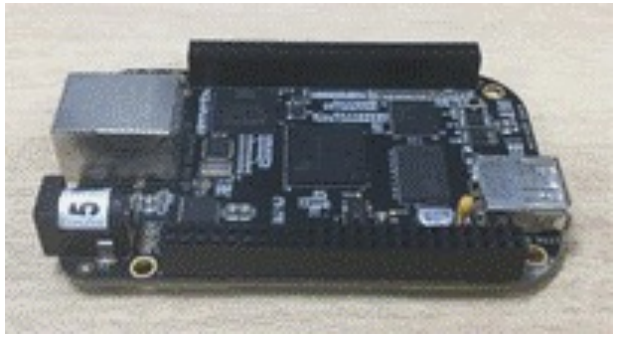
具体例

- 攻撃用端末等を通信機器等に接続し、中間者攻撃を実施
- ネットワーク機器の設定ミスや機能不備を悪用してネットワークに接続

対策例

・ARPテーブル管理可能なスイッチ導入
・ホワイトリストスイッチ導入
・制御用IDS/IPSによる検知・防御　他

参考：攻撃用不正端末に利用可能な超小型PC



ラズベリーパイ

5cm程度

10cm程度

ビーグルボーンブラック

・これらは、CPU、メモリ、ストレージ、ネットワークインタフェース、映像音声出力インタフェースをワンボード上に格納した超小型PC
・拡張モジュール装着可能であり、LTEモジュールを装着すれば、日本全国から操作可能
・電源はAC電源だけではなく、バッテリーを装着可能

・攻撃用端末として利用可能
・端末はスイッチ等の空きポートに装着

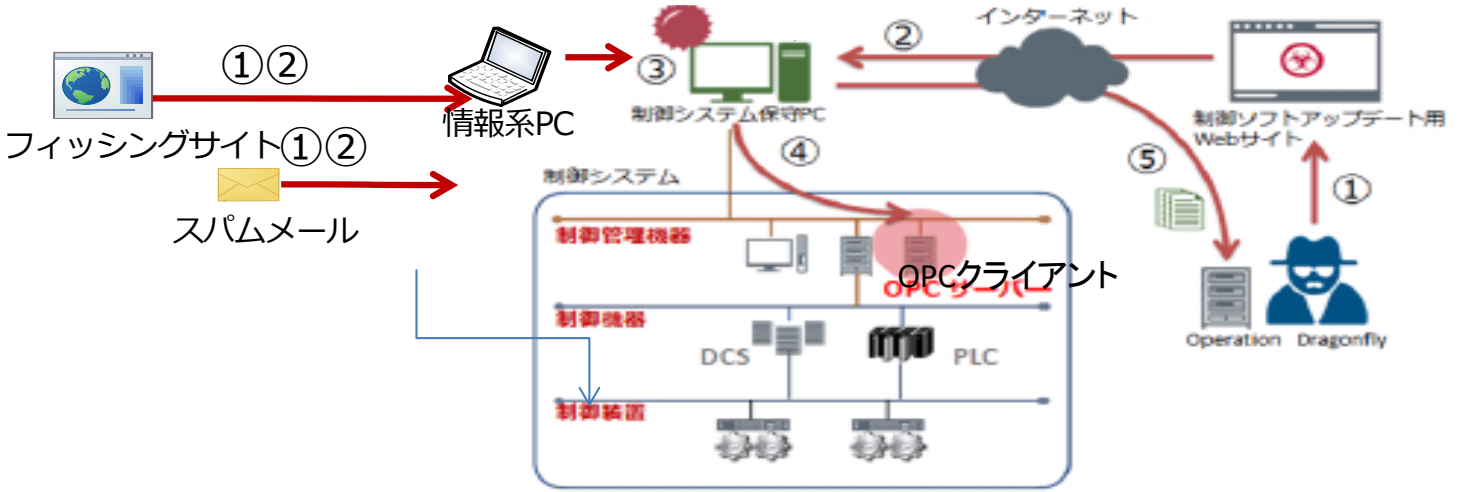
制御システムへのサイバー攻撃シナリオ(3)

情報系システムを介した攻撃

- 攻撃者はマルウェアを情報系システムを介して制御システムに侵入させ、機能不全や制御パラメータ搾取を実行

具体例

- マルウェアはインターネットから情報系PCに侵入
- 情報交換サーバやルータの脆弱性を突いて、制御システムに侵入
- マルウェアはバックドアにより制御ネットワーク内のサーバからの情報を搾取
- マルウェアは制御パラメータを改竄し、機能不全に至る攻撃を実施



注：マカフィー社＋他資料より作成

図1：Operation Dragonfly の制御システムベンダーのWebサイトを使った攻撃の仕組み（マカフィー社資料より）

対策例

- 情報交換サーバにおける脆弱性対応
- 制御ネットワーク内のDPI（Deep Packet Inspetion）ツールの導入

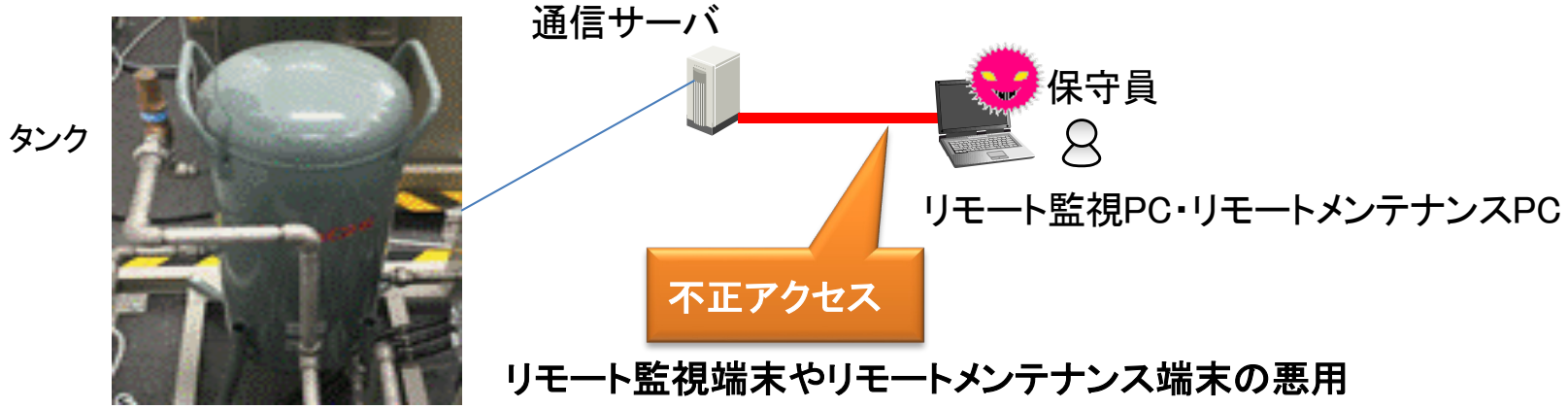
制御システムへのサイバー攻撃シナリオ(4)

リモート接続端末を用いた攻撃

- 攻撃者はリモート監視端末やリモートメンテナンス端末を用いてフィールド機器に攻撃する

具体例

- リモート保守ネットワークを悪用して内部ネットワークに侵入
- ネットワーク機器やセキュリティ機器の設定ミスや機能不備を悪用してフィールド機器に攻撃



対策例

・リモート接続端末の機器認証
・リモート接続端末の専用化
・リモート接続端末の運用に係る監査
・FWやIPS等の導入によるアクセス制限や振る舞い制限　他

チェックリスト（一部抜粋）

チェックリスト案（一部抜粋）

項番	大項目	チェック項目	重要度	コメント	評価
1-1	USBメモリ等外部記憶媒体による既知ウィルス感染				
		管理された外部記憶媒体のみ利用ルール	◎		
		USBポートの利用禁止ルール	○		
		USBポートの無効化	◎		
		持込者の申請によるウィルスチェックの確認	◎		
		外部記憶媒体等の隔離環境における最新ソフトによるウィルスチェック	◎		
		複数ウィルス対策ソフトによるウィルスチェック	◎		
		外部記憶媒体等の米国系・欧州系ウィルス対策ソフトによるウィルスチェック	○		
		端末とサーバにおけるホワイトリスト導入	○		
1-2	USBメモリ等外部記憶媒体による未知ウィルス感染				
		管理された外部記憶媒体のみ利用ルール	◎		
		USBポートの利用禁止ルール	○		
		USBポートの無効化	○		
		持込者の申請によるウィルスチェックの確認	◎		
		外部記憶媒体等の米国系・欧州系ウィルス対策ソフトによるウィルスチェック	◎		
		動的ツールによるウィルスの振る舞いチェック	◎		
		端末とサーバにおけるホワイトリスト導入	○		
1-3	持込PCによる不正侵入				
		管理されたPCのみ利用ルール	◎		
		持込者の申請によるウィルスチェックの確認	◎		
		持込PCの隔離環境における最新ソフトによるウィルスチェック	◎		
		複数ウィルス対策ソフトによるウィルスチェック	◎		
		持込PCの米国系・欧州系ウィルス対策ソフトによるウィルスチェック	◎		
		接続機器のMAC アドレス認証	◎		
		ARP Spoofing対策済のスイッチ導入	◎		
		接続機器への証明書配布	○		
		端末とサーバにおけるホワイトリスト導入	○		
		空きポートにケーブルを不正に接続できないこと	◎		
		動的ツールによるウィルスの振る舞いチェック	◎		

アウトプットイメージ

調査の総括

××××システムの特徴

1. ○○○○は事業の中核に位置し、事業継続上極めて重要なシステムである
2. ××××の目的、機能ともに他に類似がないシステムであり、設計手法・実装手法・保守管理手法等独自である

調査の総括

a. 他の重要インフラ等の制御システムと比較するとセキュリティ対策のレベルは高く、かつ過去の経験の積み重ねにより独自の対策がなされている
b. 外部ネットワークからの侵入、持込記憶媒体や持込PC等からのマルウェア感染については一応の対策がなされている
c. 物理セキュリティに関して、生体認証とICカードによる多要素認証を実現し、一定の成果を上げている
d. 対策は性善説が前提であり、内部犯行や不適切な操作等を想定されていない

攻撃シナリオ毎の評価

アウトプットイメージは以下の通り。対策優先度は、事業影響度と攻撃可能性から算出し、対策容易性は参考情報とする。

	現状の評価	事業影響度	攻撃可能性	対策優先度	対応是非	参考：対策容易性
攻撃シナリオ1	◎	9	9	81	×	9
攻撃シナリオ2	×	9	3	27	×	1
攻撃シナリオ3	○	3	3	3	○	9
攻撃シナリオ4	△	1	1	1	×	3
攻撃シナリオ5	○	6	9	54	◎	6
…						

凡例の説明

◎	対策優先度	50以上	喫緊に対応すべき
○	対策優先度	10以上	速やかに対応すべき
△	対策優先度	10未満	対応の必要性あり（対応内容を検討）

特徴：
1. 現状の対策が、何に対して（攻撃シナリオ）なされているかを明確にする
2. 本評価を繰り返すことにより、対策の充実度を測定できる

攻撃シナリオ年次評価

アウトプットイメージは以下の通り。対策優先度は、事業影響度と攻撃可能性から算出し、対策容易性は参考情報とする。

	H28	H29	H30	H31	H32	補足
攻撃シナリオ1	△	○	◎	◎	◎	
攻撃シナリオ2	×	×	×	×	△	
攻撃シナリオ3	△	○	○	◎	◎	
攻撃シナリオ4	△	△	△	△	△	
攻撃シナリオ5	×	×	△	△	△	
攻撃シナリオ6	×	×	×	×	△	
攻撃シナリオ7	×	×	×	×	×	対応せず
攻撃シナリオ8	×	×	×	×	△	
攻撃シナリオ9	×	×	△	△	△	
攻撃シナリオ10	×	×	×	×	×	
攻撃シナリオ11	×	×	×	×	△	

攻撃シナリオの評価手法(1)

攻撃シナリオ毎に、事業影響度と攻撃可能性を評価し、対策優先度を算定する。

対策優先度＝事業影響度×攻撃可能性

事業影響度　＝ MAX {信用失墜影響度、設備影響度（復旧コスト×影響範囲）}

〇信用失墜影響度
高（3）・・・直接事業継続上の脅威につながる場合
中（2）・・・直接事業継続上の脅威にはつながらないが間接的に影響を及ぼす可能性がある場合
低（1）・・・関係者の業務に軽微な影響を及ぼす場合

（復旧コスト×影響範囲が、6～9ならば設備影響度：高（3）、3～4ならば設備影響度：中（2）、1～2ならば設備影響度：低（1））

〇復旧コスト
高（3）・・・事故発生後の復旧に多大なコストを要する場合
中（2）・・・事故発生後の機器の手動再起動など復旧にコストを要する場合
低（1）・・・事故発生後の暫定的な復旧にコストを要さないが、恒久対応時にコストを要する場合

〇影響範囲
高（3）・・・事業継続上の脅威が発現する可能性が高い場合
中（2）・・・事業継続上の脅威が発現する可能性がある場合
低（1）・・・事業継続上の脅威に可能性が非常に低い場合

攻撃シナリオの評価手法(2)

攻撃可能性 ＝ 物理的な侵入の容易性 × 技術的難易度
（物理的な侵入の容易性×攻撃の容易性が、6～9ならば攻撃の可能性：高（3）、3～4ならば攻撃の可能性：中（2）、1～2ならば攻撃の可能性：低（1））

〇物理的な侵入の容易性
高（3）・・・重要施設への物理的なアクセスは不要であり、外部ネットワーク経由で攻撃可能
中（2）・・・重要施設付近に立ち入り可能なエリアで攻撃可能
低（1）・・・重要施設内へ侵入することで攻撃可能

〇技術的難易度
低（3）・・・攻撃に用いるハードウェア及びソフトウェアが容易に入手*2可能かつ対象システムに関して容易に取得*3可能な情報を用いて攻撃可能
中（2）・・・攻撃に用いるハードウェア及びソフトウェアが容易に入手*2不可能または対象システムに関して容易に取得*3不可能な情報を用いて攻撃可能
高（1）・・・攻撃に用いるハードウェア及びソフトウェアが容易に入手*2不可能かつ対象システムに関して容易に取得*3不可能な情報を用いて攻撃可能

*2・・・「容易に入手」の定義：インターネット等で比較的安価（50万円未満）に入手可能かつファームウェア書き換え等の複雑なカスタマイズが不要。
*3・・・「容易に取得」の定義：対象システムの関係者以外の不特定多数のユーザが入手可能。

攻撃シナリオの評価手法(3)

対策容易性＝対策コスト × 対策の実装期間

対策容易性＝対策コスト×対策の実施期間は以下の通り。
対策容易性　6～9:高(3)
対策容易性　3～4:中(2)
対策容易性　1～2:低(1)

〇対策コスト
高(3)・・・比較的安価(100万円未満)で対応可能
中(2)・・・中程度(100万円-1500万円未満)で対応可能
低(1)・・・大(1500万円以上)で対応可能

〇対策の実施期間
短(3)・・・決定後一週間以内に実装可能
中(2)・・・決定後1年程度で実装可能
低(1)・・・決定後数年で実装可能

対策優先度は、参考情報として記載するものとする。