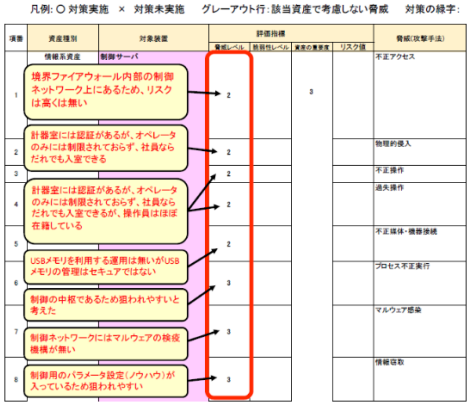
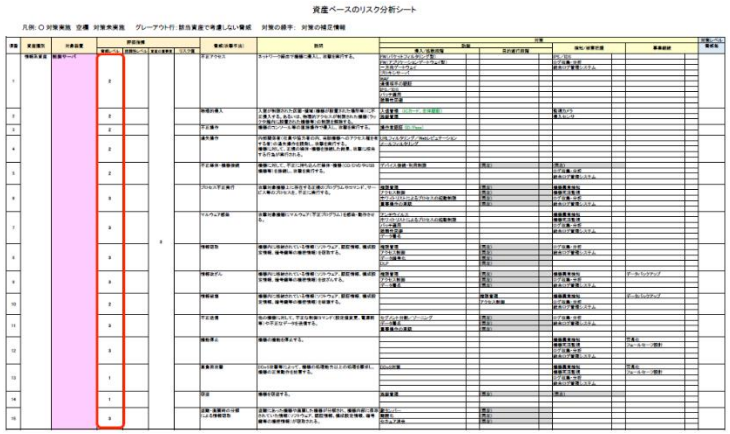
「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

<table>
<tr><th>該当箇所</th><th>2020 年 3 月版</th><th>2018 年 10 月版</th></tr>
<tr><td>p.21　表 1-1
（p.20: 2018 年 10 月版）</td><td>ガイドライン等の例を追記・修正（最新版に反映）
表 1-1 リスクアセスメントまたはリスク分析の実施を要求するガイドライン等の例
<table><tr><th>発行元</th><th>ガイドライン等の名称</th></tr><tr><td>IEC</td><td>IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program[13]</td></tr><tr><td>ISO/IEC</td><td>ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements[14]</td></tr><tr><td>NIST</td><td>Cybersecurity Framework Version 1.1 (April 2018)[15]</td></tr><tr><td>NISC</td><td>重要インフラにおける情報セキュリティ確保係る安全基準等策定指針（第 5 版）[16]</td></tr><tr><td>経済産業省</td><td>情報セキュリティ管理基準（平成 28 年改正版）[17]</td></tr><tr><td>日本電気協会</td><td>JESC Z0004(2019) 電力制御システムセキュリティガイドライン[18]</td></tr><tr><td rowspan="2">厚生労働省</td><td>医療情報システムの安全管理に関するガイドライン 第 5 版[19]</td></tr><tr><td>水道分野における情報セキュリティガイドライン 第 4 版[20]</td></tr><tr><td rowspan="4">国土交通省</td><td>鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第 4 版[21]</td></tr><tr><td>物流分野における情報セキュリティ確保に係る安全ガイドライン 第 4 版[22]</td></tr><tr><td>航空分野における情報セキュリティ確保に係る安全ガイドライン 第 5 版[23]</td></tr><tr><td>空港分野における情報セキュリティ確保に係る安全ガイドライン 第 2 版[24]</td></tr></table></td><td>表 1-1 リスクアセスメントまたはリスク分析の実施を要求するガイドライン等の例
<table><tr><th>発行元</th><th>ガイドライン等の名称</th></tr><tr><td>IEC</td><td>IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program[13]</td></tr><tr><td>ISO/IEC</td><td>ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements[14]</td></tr><tr><td>NIST</td><td>Cybersecurity Framework Version 1.1 (April 2018)[15]</td></tr><tr><td>NISC</td><td>重要インフラにおける情報セキュリティ確保係る安全基準等策定指針（第 5 版）[16]</td></tr><tr><td>経済産業省</td><td>情報セキュリティ管理基準（平成 28 年改正版）[17]</td></tr><tr><td>日本電気協会</td><td>JESC Z0004(2016) 電力制御システムセキュリティガイドライン 初版[18]</td></tr><tr><td>厚生労働省</td><td>医療情報システムの安全管理に関するガイドライン 第 5 版[19]</td></tr><tr><td rowspan="2">国土交通省</td><td>鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第 3 版[20]</td></tr><tr><td>航空分野における情報セキュリティ確保に係る安全ガイドライン 第 4 版[21]</td></tr></table></td></tr>
<tr><td>p.22　表 1-2
（p.21: 2018 年 10 月版）</td><td>ISO/IEC 27000:2018（JIS Q 27000:2019）における規定</td><td>ISO/IEC 27000:2014（JIS Q 27000:2014）における規定</td></tr>
<tr><td>p.54　表 3-6
「構築ベンダー／機器ベンダー」の説明</td><td>資産の提供元によって納入時やファームウェアアップデート等メンテナンスのポリシーが異なる場合があるので、個別に調べておく。</td><td>資産の提供元によって納入時やファームウエアアップデート等メンテナンスのポリシーが異なる場合があるので、個別に調べておく。</td></tr>
<tr><td>p.70　3.2.3.（2）
【分類 4】の説明</td><td>これら 2 段のファイアウォールの種類を別のものにしておくと、例えばファームウェアの脆弱性が露見した様な場合でも、制御ネットワークの侵入を困難にして保護することができる。</td><td>これら 2 段のファイアウォールの種類を別のものにしておくと、例えばファームウエアの脆弱性が露見した様な場合でも、制御ネットワークの侵入を困難にして保護することができる。</td></tr>
<tr><td>p.86　図 3-16</td><td>抜けていた「ルータ」を追記</td><td></td></tr>
</table>

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

該当箇所	2020 年 3 月版	2018 年 10 月版
p.145　図 5-6	名称:「**脅威レベルの記入例（一部拡大）**」 内容:シートの一部拡大して、脅威レベルの値の説明を追記 	名称:「**脅威レベルの記入例**」 内容:シート全体を記載して、脅威レベルの値の説明なし 
p.151　5.5.	評価指標「脆弱性レベル」は、…である。資産ベースのリスク分析においては、…を表す。その値は、双対の関係にある対策レベルの値から求まる。	評価指標「脆弱性レベル」は、…である。資産ベースのリスク分析においては、…を表す。その値は、対策レベルの双対の値となる。
p.152　5.5.1.	4.4.5 項において定義した通り、評価指標の一つである「脆弱性レベル」の値は、双対の関係にある「対策レベル」の値から求まる。	4.4.5 項において定義した通り、評価指標の一つである「脆弱性レベル」の値は、「対策レベル」の双対の値として定義する。
p.175　コラム	付録 C にて、制御システムのインシデント事例を紹介しているので、参考にして欲しい。	なお、本書の付録 C にて、制御システムのインシデント事例を紹介しているので、参考にして欲しい。
p.175　コラム	参考として、ドイツ連邦政府情報セキュリティ庁（BSI）がまとめたレポート“Industrial Control System Security - Top 10 Threats and Countermeasures 2019”では、制御システムに対する危険度の高い 10 大脅威とその対策が紹介されている。	参考として、ドイツの BSI（Federal Office for Information Security）がまとめたレポート“Industrial Control System Security – Top 10 Threats and Countermeasures 2016”を参照すると、Top4 は以下となる。なお、（ ）内は 2014 年の順位である。

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

<table>
<tr><th>該当箇所</th><th>2020 年 3 月版</th><th>2018 年 10 月版</th></tr>
<tr><td>p.175　コラム</td><td>10 大脅威と対策（2019 年）の 1～10 位の表を掲載
<table><tr><th colspan="2">産業用制御システムのセキュリティ 10 大脅威（2019 年）</th><th>2016 年</th></tr><tr><td>1 位</td><td>リムーバブルメディアや外部機器経由のマルウェア感染</td><td>2 位</td></tr><tr><td>2 位</td><td>インターネットおよびイントラネット経由のマルウェア感染</td><td>3 位</td></tr><tr><td>3 位</td><td>ヒューマンエラーと妨害行為</td><td>5 位</td></tr><tr><td>4 位</td><td>外部ネットワークやクラウドコンポーネントへの攻撃</td><td>8 位</td></tr><tr><td>5 位</td><td>ソーシャルエンジニアリングとフィッシング</td><td>1 位</td></tr><tr><td>6 位</td><td>DoS/DDoS 攻撃</td><td>9 位</td></tr><tr><td>7 位</td><td>インターネットに接続された制御機器</td><td>6 位</td></tr><tr><td>8 位</td><td>リモートアクセスからの侵入</td><td>4 位</td></tr><tr><td>9 位</td><td>技術的な不具合と不可抗力</td><td>7 位</td></tr><tr><td>10 位</td><td>スマートデバイスへの攻撃</td><td>10 位</td></tr></table></td><td>10 大脅威と対策（2016 年）の 1～4 位の表を掲載
<table><tr><th>【順位】</th><th>【内容】</th></tr><tr><td>1（3）</td><td>ソーシャルエンジニアリングとフィッシング</td></tr><tr><td>2（2）</td><td>外部記憶媒体または外付けハードウェア（ノート PC 等）経由のマルウェア感染</td></tr><tr><td>3（1）</td><td>インターネットおよびイントラネットからのマルウェア感染</td></tr><tr><td>4（5）</td><td>リモートアクセスからの侵入</td></tr></table></td></tr>
<tr><td>p.175　コラム</td><td>あくまで海外事例ではあるが、これを見ると、上位 4 位は全て順位が上昇しており、制御システムに対する攻撃手法の変遷が見て取れる。1 位の「外部記憶媒体または外付けハードウェア経由のマルウェア感染」、2 位の「インターネットおよびイントラネットからのマルウェア感染」は、いずれも典型的かつ重要な脅威として取り上げ、攻撃ツリー選定時に参考にして欲しい。</td><td>あくまで海外事例ではあるが、これを見ると、1 位と 3 位が入れ替わっており、制御システムに対する攻撃手法の変遷が見て取れる。また、2 位の「外部記憶媒体または外付けハードウェア経由のマルウェア感染」、3 位の「インターネットおよびイントラネットからのマルウェア感染」、4 位の「リモートアクセスからの侵入」は、いずれも典型的かつ重要な脅威として取り上げ、攻撃ツリー選定時に参考にして欲しい。</td></tr>
<tr><td>p.217　表 6-20
「対策」の説明</td><td>対策（「侵入段階」、「目的遂行段階」、「検知・被害把握」、「事業継続」）及び対策状況を記入する欄。対策及び対策状況は攻撃ステップ単位で記入する。</td><td>対策（「侵入段階」、「目的遂行段階」、「検知・被害把握」、「事業継続」）および対策状況を記入する欄。対策および対策状況は攻撃ステップ単位で記入する。</td></tr>
</table>

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

該当箇所	2020 年 3 月版	2018 年 10 月版
p.233　6.10.	評価指標「セキュリティ対策状況」の評価値「対策レベル」は、…である。事業被害ベースのリスク分析においては、攻撃ステップ及び攻撃ツリーについて対策レベルの評価を行い、**想定した攻撃（攻撃ステップ、攻撃ツリー）が発生した場合、現在実施している対策で防止できる可能性**を表す。	評価指標「セキュリティ対策状況」の評価値「対策レベル」は、…である。事業被害ベースのリスク分析においては、攻撃ステップの対策レベルの評価と攻撃ツリーの対策レベルの評価の 2 段階で行い、**想定した攻撃（攻撃ステップ、攻撃ツリー）が発生した場合、現在実施している対策で防止できる可能性**を表す。
p.233　6.10.	評価指標「脆弱性」の評価値「脆弱性レベル」は、…である。事業被害ベースのリスク分析においては、攻撃ツリーについて脆弱性レベルの評価を行い、**想定する攻撃ツリーが発生した場合、それを受け入れてしまう可能性、即ち、攻撃が成功する可能性**を表す。その値は、双対の関係にある攻撃ツリーの対策レベル値から求まる。	評価指標「脆弱性」の評価値「脆弱性レベル」は、…である。事業被害ベースのリスク分析においては、攻撃ツリーの脆弱性レベルの評価の 1 段階のみを行い、**想定する攻撃ツリーが発生した場合、それを受け入れてしまう可能性、即ち、攻撃が成功する可能性**を表す。その値は、攻撃ツリーの対策レベルの双対の値となる。
p.237　6.10.2.	攻撃ツリーの脆弱性レベルの値は、双対の関係にある攻撃ツリーの対策レベルの値から算出し、事業被害ベースのリスク分析シートの「評価指標」の「脆弱性レベル」欄に記入する。	脆弱性レベルは、攻撃ツリーの対策レベルの双対の値を、事業被害ベースのリスク分析シートの「評価指標」の「脆弱性レベル」欄に記入する。
p.258　7.1.2. 項末に文章を追記	また、資産の重要度、脅威レベル、脆弱性レベルの各評価値の組み合わせによっては、対策の強化により脆弱性レベルを下げても、リスク値は変化しない（見かけ上、リスクが低減されない）ことがあるので、注意が必要である。巻末（p.381）の追加コラム**「見かけ上、低減されないリスク」**に、詳細の説明を記載する。	
p.259　コラム タイトル	**攻撃過程を考慮した対策検討箇所の抽出（資産ベース分析版）**	**攻撃過程を考慮した対策検討箇所の抽出**

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

<table>
<tr><th>該当箇所</th><th>2020 年 3 月版</th><th>2018 年 10 月版</th></tr>
<tr><td>p.261　7.1.3.</td><td>資産ベースのリスク分析シート（図 7 2）では、…を検討する。例えば、…を追加実施する。その結果、対策レベルと双対の関係にある、評価指標「脆弱性レベル」（図中④）を 3→2 に低減することで、リスク値が A→B に低減される。</td><td>資産ベースのリスク分析シート（図 7 2）では、…を検討する。例えば、…を追加実施する。その結果、対策レベルの双対の値である、評価指標「脆弱性レベル」（図中④）を 3→2 に低減することで、リスク値が A→B に低減される。</td></tr>
<tr><td>p.261　7.1.3.</td><td>資産ベースのリスク分析結果を活用した追加対策の検討表の例を、表 7 1 に示す。本表は、…を記している。例えば、図 7 2 の対策③は本表の No.1 に対応する。</td><td>資産ベースのリスク分析結果を活用した追加対策の検討表の例を、表 7 1 に示す。本表は、…を記している。例えば、図 7 2 の対策③は本表の No.2 に対応する。</td></tr>
<tr><td>p.262　表 7-1</td><td>項目「評価」「実現可能性（運用への影響、可用性への影響）」を追加し、内容修正
表 7-1 資産ベースのリスク分析結果を活用した追加対策の検討表例（一部抜粋）
<table>
<tr><th rowspan="2">No.</th><th rowspan="2">資産名</th><th rowspan="2">高リスク値の脅威</th><th rowspan="2">想定される対策</th><th colspan="2">リスク値</th><th colspan="2">改善方法</th><th colspan="3">評価</th><th rowspan="2">実現可能性</th><th rowspan="2">優先度</th><th rowspan="2">改善実施</th><th rowspan="2">備考</th></tr>
<tr><th>対策前</th><th>対策後</th><th>システム</th><th>運用</th><th>推定対策コスト</th><th>運用への影響</th><th>可用性への影響</th></tr>
<tr><td>1</td><td rowspan="3">制御サーバ</td><td>不正媒体・機器接続</td><td>デバイス接続・利用制限</td><td>A</td><td>B</td><td>○</td><td></td><td>低</td><td>低</td><td>低</td><td>高</td><td>高</td><td>○</td><td></td></tr>
<tr><td>2</td><td>プロセス不正実行</td><td>ホワイトリストによるプロセスの起動制限</td><td>A</td><td>B</td><td>○</td><td></td><td>高</td><td>低</td><td>高</td><td>低</td><td>低</td><td>×</td><td>十分な検証が必要</td></tr>
<tr><td>3</td><td>不正送信</td><td>重要操作の承認</td><td>A</td><td>B</td><td>○</td><td>○</td><td>低</td><td>中</td><td>中</td><td>中</td><td>高</td><td>○</td><td></td></tr>
<tr><td>4</td><td rowspan="3">HMI（操作端末）</td><td>不正操作</td><td>操作者認証</td><td>A</td><td>B</td><td>○</td><td>○</td><td>高</td><td>中</td><td>高</td><td>低</td><td>低</td><td>×</td><td>ソフトウェアの改造必要</td></tr>
<tr><td>5</td><td>不正送信</td><td>重要操作の承認</td><td>A</td><td>B～C</td><td>○</td><td></td><td>高</td><td>低</td><td>高</td><td>低</td><td>低</td><td>×</td><td>十分な検証が必要</td></tr>
<tr><td>6</td><td>情報改ざん</td><td>権限管理／アクセス制御</td><td>A</td><td>B</td><td>○</td><td></td><td>低</td><td>低</td><td>低</td><td>高</td><td>高</td><td>○</td><td></td></tr>
</table></td><td>表 7-1 資産ベースのリスク分析結果を活用した追加対策の検討表例（一部抜粋）
<table>
<tr><th rowspan="2">No.</th><th rowspan="2">資産名</th><th rowspan="2">高リスク値の脅威</th><th rowspan="2">リスク値</th><th rowspan="2">想定される対策</th><th rowspan="2">「効果」対策後リスク値</th><th rowspan="2">推定対策コスト</th><th colspan="2">改善方法</th><th rowspan="2">優先度</th><th rowspan="2">改善実施</th><th rowspan="2">備考</th></tr>
<tr><th>システム</th><th>運用</th></tr>
<tr><td>1</td><td rowspan="3">制御サーバ</td><td>不正媒体・機器接続</td><td>A</td><td>デバイス接続・利用制限</td><td>B</td><td>低</td><td>○</td><td></td><td>高</td><td>○</td><td></td></tr>
<tr><td>2</td><td>プロセス不正実行</td><td>A</td><td>ホワイトリストによるプロセスの起動制限</td><td>B</td><td>高</td><td>○</td><td></td><td>低</td><td>×</td><td>十分な検証が必要</td></tr>
<tr><td>3</td><td>不正送信</td><td>A</td><td>重要操作の承認</td><td>B</td><td>低</td><td>○</td><td>○</td><td>高</td><td>○</td><td></td></tr>
<tr><td>4</td><td rowspan="3">HMI（操作端末）</td><td>不正操作</td><td>A</td><td>操作者認証</td><td>B</td><td>高</td><td>○</td><td>○</td><td>低</td><td>×</td><td>ソフトウェアの改造必要</td></tr>
<tr><td>5</td><td>プロセス不正実行</td><td>A</td><td>ホワイトリストによるプロセスの起動制限</td><td>B～C</td><td>高</td><td>○</td><td></td><td>低</td><td>×</td><td>十分な検証が必要</td></tr>
<tr><td>6</td><td>情報改ざん</td><td>A</td><td>権限管理／アクセス制御</td><td>B</td><td>低</td><td>○</td><td></td><td>高</td><td>○</td><td></td></tr>
</table></td></tr>
<tr><td>p.263　7.1.4.</td><td>図 7 5 に、…を記す。この様に、システム全体のリスク値の改善効果を把握するには、リスク値ごとのヒストグラムを作成するとわかりやすい。</td><td>図 7 5 に、…を記す。この様に、システム全体のリスク値の改善効果を把握するには、リスク値ごとのヒストグラムを作成するのがわかりやすい。</td></tr>
</table>

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

<table>
<tr><th>該当箇所</th><th>2020 年 3 月版</th><th>2018 年 10 月版</th></tr>
<tr><td>p.272　表 7-3</td><td>項目「脅威」「リスク値」「評価」「実現可能性（運用への影響、可用性への影響）」を追加し、内容修正
表 7-3 事業被害ベースのリスク分析結果対策表の例
<table>
<tr><th rowspan="2">項番</th><th rowspan="2">攻撃ツリー概要</th><th rowspan="2">想定されるシナリオ</th><th rowspan="2">対策箇所</th><th rowspan="2">脅威</th><th rowspan="2">想定される対策</th><th colspan="2">リスク値</th><th colspan="2">改善方法</th><th colspan="3">評価</th><th rowspan="2">実現可能性</th><th rowspan="2">優先度</th><th rowspan="2">改善実施</th><th rowspan="2">備考</th></tr>
<tr><th>対策前</th><th>対策後</th><th>システム</th><th>運用</th><th>推定対策コスト</th><th>運用への影響</th><th>可用性への影響</th></tr>
<tr><td>1, 14</td><td>悪意の第三者：監視端末→2 台のデータヒストリアン経由で HMI を攻撃</td><td>データヒストリアンの脆弱性を利用し侵攻、HMI を遠隔操作</td><td>データヒストリアン（中継）</td><td>不正アクセス</td><td>パッチの適用（即時）</td><td>B</td><td>C</td><td>○</td><td></td><td>低</td><td>高</td><td>中</td><td></td><td></td><td></td><td>パッチ適用はベンダーと要相談</td></tr>
<tr><td>6</td><td>内部関係者（過失）：USB 経由で HMI がマルウェアに感染</td><td>USB メモリ持ち込みで HMI がマルウェア感染</td><td>HMI</td><td>不正媒体・機器接続</td><td>USB 持込禁止／USB ポートロック</td><td>A</td><td>B</td><td>○</td><td>○</td><td>低</td><td>低</td><td>低</td><td>高</td><td>高</td><td>○</td><td></td></tr>
<tr><td>10</td><td>悪意の第三者：FW を超えて EWS を不正操作</td><td>FW の脆弱性を利用し突破、コントローラから供給停止</td><td>FW</td><td>不正アクセス</td><td>パッチの適用（即時）</td><td>B</td><td>C</td><td>○</td><td></td><td>中</td><td>中</td><td>低</td><td>高</td><td></td><td>○</td><td></td></tr>
<tr><td>19, 28</td><td>内部関係者（過失）：USB 経由で EWS がマルウェアに感染</td><td>USB メモリ持ち込みで EWS がマルウェア感染</td><td>EWS</td><td>不正媒体・機器接続</td><td>USB ポートロック（使用時のみ解錠）</td><td>A</td><td>B</td><td>○</td><td>○</td><td>低</td><td>高</td><td>中</td><td></td><td></td><td></td><td>利用時 USB ウイルスチェック（運用改善）も検討</td></tr>
</table></td><td>表 7-3 事業被害ベースのリスク分析結果対策表の例
<table>
<tr><th rowspan="2">#</th><th rowspan="2">攻撃ツリー概要</th><th rowspan="2">想定されるシナリオ</th><th rowspan="2">対策箇所</th><th rowspan="2">想定される対策</th><th rowspan="2">推定対策コスト</th><th colspan="2">改善方法</th><th rowspan="2">優先度</th><th rowspan="2">改善実施</th><th rowspan="2">備考</th></tr>
<tr><th>システム</th><th>運用</th></tr>
<tr><td>1</td><td>内部関係者（過失）：USB 経由で EWS がマルウェアに感染</td><td>USB メモリ持ち込みで EWS がマルウェア感染</td><td>EWS</td><td>USB ポートロック</td><td>低</td><td>○</td><td></td><td>高</td><td>○</td><td></td></tr>
<tr><td>2</td><td>内部関係者（過失）：HMI からシステムの停止操作の実行</td><td>HMI から停止コマンドを騙って送信する</td><td>HMI</td><td>重要操作の承認</td><td>中</td><td>○</td><td>○</td><td>低</td><td></td><td>運用の検討要</td></tr>
<tr><td>3</td><td>悪意の第三者：監視端末～2 台のデータヒストリアン経由で HMI 攻撃</td><td>データヒストリアンの脆弱性を利用し侵攻、HMI を遠隔操作</td><td>データヒストリアン</td><td>パッチの適用</td><td>低</td><td>○</td><td></td><td>高</td><td>○</td><td></td></tr>
<tr><td>4</td><td>悪意の第三者：FW を超えて EWS の情報窃取</td><td>FW の脆弱性を利用し突破、EWS の情報を窃取</td><td>EWS</td><td>データの暗号化</td><td>中</td><td>○</td><td></td><td>低</td><td></td><td>動作検証要</td></tr>
</table></td></tr>
<tr><td>p.309　参考文献</td><td>IEC/TS 62443-1-1: 2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models</td><td>IEC/TS 62443-1-1: 2009, Industrial communication networks - Network ans system security - Part 1-1: Terminology, concenpts and models</td></tr>
<tr><td>p.315　A.3.</td><td>CPNI（Centre for the Protection of National Infrastructure）が…</td><td>CPNI（Centre for the Protection of National Inftrastracture）が…</td></tr>
<tr><td>p.351　B.4.2.　項番 32</td><td>Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).</td><td>Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).</td></tr>
<tr><td>p.361　付録 C　項番 2</td><td>http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf
（p.73）（公開終了）</td><td>http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf
（p.73）</td></tr>
</table>

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

該当箇所	2020 年 3 月版	2018 年 10 月版
p.361　付録 C　項番 3	http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf (p.75)（公開終了）	http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf (p.75)
p.361　付録 C　項番 6	（リンク切れのため削除）	http://www.npa.go.jp/keibi/biki3/20120919kouhou.pdf
p.362　付録 C　項番 7	http://www.nids.mod.go.jp/event/proceedings/symposium/pdf/2016/j_02.pdf	http://www.nids.mod.go.jp/event/symposium/pdf/2016/j_02.pdf
p.363　付録 C　項番 13	（リンク切れのため削除）	http://www.techweekeurope.co.uk/security/cyberwar/steelworks-damaged-cyber-attack-158107
p.363　付録 C　項番 15	https://www.csoonline.com/article/2968432/cyber-physical-attacks-hacking-a-chemical-plant.html	http://nationalcybersecurity.com/cyber-physical-attacks-hacking-a-chemical-plant/
p.364　付録 C　項番 22	https://www.eweek.com/security/embedded-windows-medical-devices-infected-by-wannacry-ransomware	http://www.eweek.com/security/embedded-windows-medical-devices-infected-by-wannacry-ransomware
p.365　付録 C　項番 27	https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack	http://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack
p.365　付録 C　項番 28	（サイト閉鎖のため削除）	https://www.theinquirer.net/inquirer/news/3037125/tsmc-says-wannacry-forced-factory-shutdown

「制御システムのセキュリティリスク分析ガイド　第2版」（2020 年 3 月版） 変更箇所一覧

2020 年 3 月 16 日
独立行政法人情報処理推進機構

該当箇所	2020 年 3 月版	2018 年 10 月版
p.366　付録 C.	制御システムのインシデント事例一覧の 6 ページ目（項番 29～33）を追加 	
p.375　付録 D　HSE	健康（Health）、…	健康（Heaith）、…
p.376　付録 E.	第 2 版では、攻撃が成功した場合の事業被害が大きく、攻撃者に狙われる可能性が高い重要な攻撃ツリーを選定して、優先的に分析を行うことで、分析の有用性を確保しつつ事業者が投入可能な人員及び予算で実施できるよう、分析の方法を見直した。	第 2 版では、攻撃が成功した場合の事業被害が大きく、攻撃者に狙われる可能性が高い重要な攻撃ツリーを選定して、優先的に分析を行うことで、分析の有用性を確保しつつ事業者が投入可能な人員および予算で実施できるよう、分析の方法を見直した。
p.379-380　追加コラム	【追加コラム（5.5.1 項＆6.10.1 項）】「攻撃者の損益分岐点を考慮した対策レベルの評価」を追記	
p.381　追加コラム	【追加コラム（7.1.2 項）】「見かけ上、低減されないリスク」を追記	
p.382　追加コラム	【追加コラム（7.2.2　項）】「攻撃過程を考慮した対策検討脅威の抽出（事業被害ベース分析版）」を追記	
p.383　更新履歴	2020 年 3 月版（2020 年 3 月 16 日公開）の履歴を追記	