CSSCのペネトレーションテスト

2020年12月

技術研究組合制御システムセキュリティセンター

CSSCのペネトレーションテストの特徴

対象

1. 制御システムや制御機器（スマートメーターシステムや関連機器を含む）を対象
2. ブラックボックステストを基本とし、あらゆるプロトコル種別を対象
3. 有線イーサネットだけではなく、無線系やシリアル通信も対応可能
4. IPv4だけではなくIPv6、産業用イーサネット通信プロトコルの検証にも対応可能

検証手法の特徴

1. CSSCが有する検証技術により可能な範囲で脆弱性を抽出する
2. 脆弱性やパラメータチューニング、組み合わせなど独自のノウハウを用いて実施
3. 想定脅威を再現するために、必要に応じて保有ツールのカスタマイズやツールの新規製作を実施し
4. ネットワークを介したテストとともに耐タンパー関連テストも実施可能

その他

1. ツールベンダーとのコネクションを有しており、対応プロトコル追加等についても正常データのエミュレーションや検証パケット作成に柔軟に対応
2. 発見した脆弱性については複数の対策案を合わせて提案
3. WebサイトやWebアプリケーション等への対応も可能

〇有線系のツールと特徴

1. 有線系のツールは、nmapやmetasploit等のフリーソフト、nessusやBrekingPoint等の商用ソフト、自作ツールを保有
2. 正常な情報系、制御系プロトコルのトラフィックを模擬しつつ、各種サイバー攻撃トラフィックのエミュレーションをおこなうことで、CPU使用率の頭打ちなどによる処理落ちなど現実的な検証が可能

〇無線系のツールと特徴

1. 無線系のツールは、パケットキャプチャドングルやスペクトラムアナライザ　評価用の無線デバイスのカスタマイズ品を保有
2. 電波暗箱を利用し、無線設備規則等に縛られないテストも実施可能

利用する検証関連ツール（一部）

製造元	CMエンジニアリング
品名	CRESSON-MD920
機能	920MHz無線トランシーバ
用途	920MHz無線ネットワークに対する不正パケットの送信

製造元	FXC
品名	ES1008MTP2
機能	パケット・フラッディング機能（リピータ）
用途	FANユニットとWANユニット間ネットワークトラフィックの盗聴及び不正パケットの送信

製造元	Analog Devices
品名	EVAL-ADF7xxxMB4Z Rev B
機能	920MHz無線トランシーバ
用途	ARIB-T108の送信時間制限を無視した電波の送信

製造元	ROHM
品名	BP35A1、BP35A7、BP359C
機能	Wi-SUN対応無線トランシーバ
用途	920MHz無線ネットワーク（Wi-SUN）に対する不正パケットの送信

製造元	KEYSIGHT
品名	W10120A
機能	920MHz無線レシーバ
用途	920MHz無線ネットワークパケットの受信及びWiresharkによるパケット解析

製造元	Ixia
品名	Breaking Point
機能	テストトラフィックジェネレータ
用途	FANユニットとWANユニット間ネットワークから不正パケットの送信

事前準備

1)脅威の特定
　御社とCSSCで打ち合わせを重ね、脅威の特定を行います。
脅威の特定とは、「制御システムにおいて、何が発生すると問題か」に関して、お互いの認識を共有することです。
同時に、攻撃方法（主として物理攻撃の関与の度合い）に関しても議論させて頂きます。

2)検証範囲の特定
　脅威の特定の結果を踏まえ、検証範囲を明確化します。
一般には、システム構成図概要版をもとに、検証対象となるサブシステムの特定を行います。

3)検証環境構築
　検証範囲の明確化終了後に、検証環境構築を行います。検証環境は御社に構築頂くか、すでに構築されているテスト用等の検証環境を利用することも一般的です。

検証作業

1)事前検証1（既存ツールを用いた検証）
　Nmap、Nessus、Metasploitを用いて情報収集を行います。並行して開示情報から、システム構成・チップ情報等を収集します。さらには、これらの情報収集により得られたシステム構成図を作成します。

2)事前検証2（CSSC独自のプロトコル検証）
　PPS限界測定、TCP header smurf、TCP不正pktサイズ攻撃、ARP spoofing、マルチキャスト攻撃等による検証を行います。さらには、制御ネットワーク部分のパケットをモニタリングし、プロトコルやパラメータの推定等を行います。

3)攻撃シナリオの検討とツールの製作
　1)の脅威を前提として、2)の結果を用いて攻撃シナリオを検討致します。必要に応じて、ツールの製作を行います。

4)本検証作業
　3)で作成した攻撃シナリオに関して、検証作業を行います。脆弱性が発見できない場合、4)に戻り攻撃シナリオの検討とツールの製作を再度行います。

過去の主な実績

年度	実績
2013	• 組合員3社のコントローラのセキュリティ評価 • ビル模擬システムAに対するセキュリティ評価 • ガス模擬プラントに対するセキュリティ評価
2014	• 組合員3社のコントローラのセキュリティ評価
2015	• 組合員3社のコントローラのセキュリティ評価 • 電力会社4社のスマートメーター通信システムに対するセキュリティ評価 • 変電模擬プラントのセキュリティ評価 • ビル模擬システムBに対するセキュリティ評価
2016	• 監視カメラシステムのセキュリティ評価 • 電力会社3社のスマートメーター通信システムに対するセキュリティ評価 • A株式会社の制御機器に対するセキュリティ評価 • B株式会社の制御システム対応ネットワーク機器に対するセキュリティ評価
2017	• 電力会社3社のスマートメーター通信システムに対するセキュリティ評価 • A株式会社の制御機器に対するセキュリティ評価
2018	• 電力会社1社のスマートメーター通信システムに対するセキュリティ評価 • C株式会社のセキュリティ機器の機能評価 • 入退室システムのセキュリティ評価
2019	• 電力会社2社のスマートメーター通信システムに対するセキュリティ評価 • A株式会社のセキュリティ機器の機能評価

アウトプット

1)脆弱性の評価
　検証作業にて発見された脆弱性を、発生確率・被害の大きさ・対応コストの観点から評価し、脆弱性の対策優先度を明示。

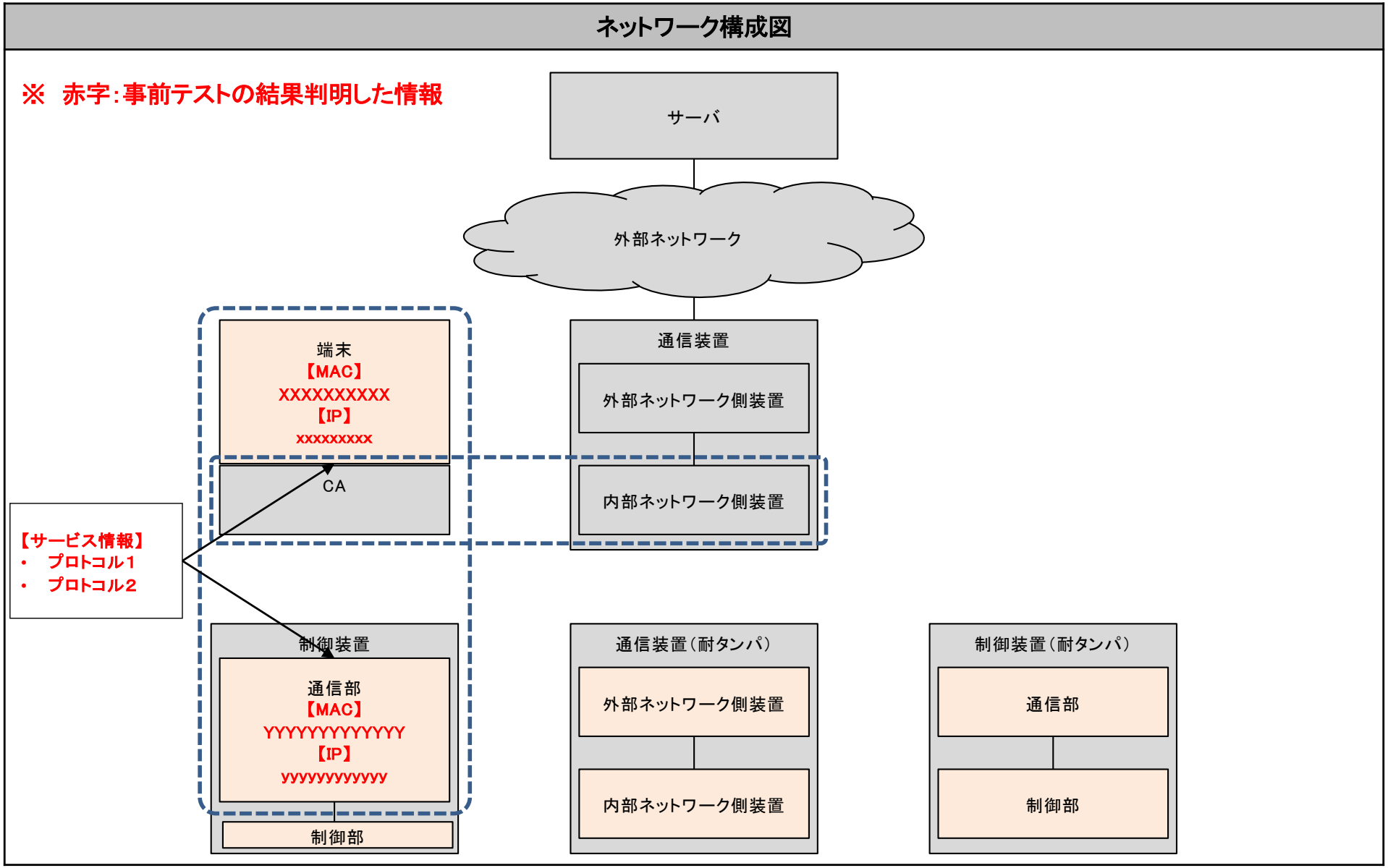
2)対策の検討
　対策に関して、以下の観点から提示。
・ソフトウェアやハードウェアの変更内容
・ネットワークやサーバ等の設定変更内容
・運用や物理セキュリティでの対応内容

3)アウトプット
　検証結果をまとめた報告書一式を納品。なお、脆弱性を発見した場合、可能な限り対策を記載。

報告書の目次例

1. 目的
2. 実施方針
3. テスト環境
4. テストツール
5. 事前テスト結果
6. 本番テスト結果
7. 耐タンパ性テスト結果
8. 脆弱性評価軸
9. 脆弱性評価結果
10. 総括

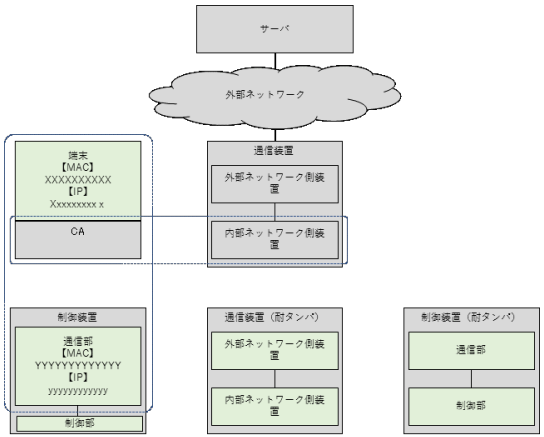
事前テスト結果（例）


ネットワーク構成図
※ 赤字：事前テストの結果判明した情報
サーバ
外部ネットワーク
通信装置
外部ネットワーク側装置
内部ネットワーク側装置
端末
【MAC】
XXXXXXXXXX
【IP】
xxxxxxxxx
CA
【サービス情報】
・ プロトコル1
・ プロトコル2
制御装置
通信部
【MAC】
YYYYYYYYYYYY
【IP】
yyyyyyyyyyy
制御部
通信装置（耐タンパ）
外部ネットワーク側装置
内部ネットワーク側装置
制御装置（耐タンパ）
通信部
制御部

本番テスト結果（例）

テストID	本番テスト
テスト名	XXXXプロトコルによる認証妨害
テスト概要	特定パケットを端末へ連続的に送信することにより、認証を妨害する。
テスト対象箇所	端末

テスト機材とトラフィック



テスト手法

① テストPCから特定パケットを端末へ連続的に送信する。
② 端末から制御装置へ認証を数回行い、端末の画面を確認する。

テスト結果確認方法

端末にエラーを示す画面が表示されるかを確認する。

テスト結果

- 制御装置通信部との接続失敗を示すポップアップが端末の画面に表示されることを確認した。
- テスト実施中に端末から操作を実行し、通信内容を確認したところ、認証関連通信が全く流れないことを確認した。
- 略

考察

特定パケットによるサービス拒否の脆弱性が存在すると推測される。

脆弱性評価軸（例）

脆弱性評価では、CSSCが定義する以下の脆弱性評価軸を基にして評価した。

緊急度＝事業影響度×攻撃の可能性（高：6または9、中：3または4、低：1または2）

事業影響度＝復旧コスト×影響範囲
（復旧コスト×影響範囲が、6または9ならば事業影響度：高（3）、3または4ならば事業影響度：中（2）、1または2ならば事業影響度：低（1））

〇復旧コスト
高（3）・・・その他復旧に多大なコストを要する場合
中（2）・・・機器の手動再起動など復旧にコストを要する場合
低（1）・・・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）・・・攻撃に用いるハードウェア単体でシステム全体に何らかの影響を及ぼす場合
中（2）・・・攻撃に用いるハードウェア単体でシステムの複数の機器に何らかの影響を及ぼす場合
低（1）・・・攻撃に用いるハードウェア単体でシステムの機器単体に何らかの影響を及ぼす場合

攻撃の可能性＝物理的な侵入の必要性×攻撃の容易性
（物理的な侵入の必要性×攻撃の容易性が、6または9ならば攻撃の可能性：高（3）、3または4ならば攻撃の可能性：中（2）、1または2ならば攻撃の可能性：低（1））

〇物理的な侵入の必要性
低（3）・・・物理的なアクセスは不要であり、無線で攻撃可能
中（2）・・・広域的に配置された通信装置または制御装置へ物理的にアクセスすることで攻撃可能
高（1）・・・事業者敷地内へ侵入することで攻撃可能

〇攻撃の容易性
高（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*1可能かつ対象システムに関して容易に取得*2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*1不可能または対象システムに関して容易に取得*2不可能な情報を用いて攻撃可能
低（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*1不可能かつ対象システムに関して容易に取得*2不可能な情報を用いて攻撃可能

*1・・・「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
*2・・・「容易に取得」の定義：事業者関係者以外の不特定多数のユーザが入手可能

脆弱性評価結果（例）

件名	特定パケットの連続送信による端末と制御装置間の認証妨害に関する脆弱性	
概要	特定パケットを端末に対して連続的に送信することにより、端末と制御装置間の認証を妨害することが可能となる。	
影響	端末を使用した制御の情報取得がなされる他、制御装置の操作ができなくなる。	
事業影響度	復旧コスト：**低（1）** × 影響範囲：**低（1）** ＝ **1** … **事業影響度：低（1）**	
攻撃の可能性	物理的な侵入の必要性（※1）：**低（3）** × 攻撃の容易性（※2）：**中（2）** ＝ **6** … **攻撃の可能性：高（3）** ※1　対象機器への物理的なアクセスは不要であり、無線で攻撃可能である。 ※2　特定パケットを送信可能なツールは独自に準備する必要があり、容易に入手することは困難である。	
緊急度	事業影響度：**低（1）** × 攻撃の可能性：**高（3）** = **3** … **緊急度：中**	
対策例	運用レベルでの対策	• サーバ側での端末や制御装置のモニタリングを綿密に実施する。
	システムレベルでの対策	なし
	機器レベルでの対策	• 特定パケットのDoS攻撃を考慮した通信部のファームウェアに更新する。

総括（例）

- 制御システムを対象としたセキュリティ評価（実機を用いたテストおよびテスト結果に基づく脆弱性評価）を実施した。

- 新規対象評価結果より、XX件の脆弱性と思われる事象（緊急度高：0件、緊急度中：XX件、緊急度低：0件）を確認した。

- 発見された脆弱性は、即時的に広範囲に影響を及ぼすものではないが、システム稼動環境や運用体制を鑑みた詳細なリスク分析の実施、および機器レベル・システムレベル・運用レベルでの対策の検討を推奨する。