そのカメラ、 正しく設定できていますか？

インターネットに接続されたカメラは第三者が簡単に見つけることができます

インターネットからアクセス可能なカメラは、検索サイトを使って探し出すことが可能です。その検索結果から脆弱性のあるカメラを自動で洗い出すツールも確認されています。
必要で無い限り IP カメラをインターネットに接続しないようにしましょう。

IP カメラへの不正アクセスがニュースになりました

【原因は初期パスワードのまま利用していたこと】
IP カメラの操作には、通常パスワードが要求されます。このパスワードが初期値のままになっていると、製品マニュアルの情報を参照できるすべての人がIPカメラを不正に操作できます。

また、IP カメラの普段使わないサーバ機能を動作させていると、それらを悪用されてマルウェアに感染することがあります。マニュアルを見て不要なサーバ機能は停止しましょう。

更に、IP カメラには利用者が停止できないバックドアと言われる侵入口が存在する場合があります。バックドアが発見されると、それを塞いだ新しいバージョンのファームウェアが製品のサイトに公開されます。設置する IP カメラが最新のファームウェアかどうかを確認しましょう。

IP カメラ安全利用のためのチェックリスト

- ☐ むやみに IP カメラをインターネットに接続しない
- ☐ IP カメラにログインできるパスワードは初期値から変更する
- ☐ Web 以外の不要なサーバ機能は停止する
- ☐ IP カメラの製品サイトを確認し、バージョンアップする

IP カメラを導入するときは、これ以外にも接続元の制限や正しく動いていることの確認など、設置や運用において気を付けなければいけないことがあります。

詳しくは、IPA で公開している、
「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」
を参照してください。

https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/checklist_nwc.pdf

IPA 独立行政法人情報処理推進機構
特定用途機器情報セキュリティ対策検討委員会

JISEC-PROC-2018-A03

JISEC-PROC-2018-A01

ネットワークカメラシステムにおける
情報セキュリティ対策要件チェックリスト

第2版

独立行政法人情報処理推進機構
特定用途機器情報セキュリティ対策検討委員会

目　　次

改版履歴

版数	発行年月日	備考
1.0	2017 年 12 月 7 日	初版発行
2.0	2018 年 3 月 30 日	アナログカメラ及びインターネット接続に対応　セキュリティ要件の一部改訂

1. はじめに

本書「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」は、「政府機関の情報セキュリティ対策のための統一基準」[1]において調達・運用時のセキュリティ要件を求められている特定用途機器のひとつである「ネットワークカメラシステム」について、想定される脅威に対策を講ずる情報セキュリティ対策の要件を列挙した資料です。政府機関や自治体に限らず、「3.1 対象とする利用形態」に該当するシステムであれば参照可能です。

本書に記載したチェックリストの各項目は、現行のネットワークカメラシステムで使われている機器の機能性を考慮した上で、現実的で適用可能なセキュリティ対策要件を具体的に記載したものです。本書が調達仕様策定時[2]や、運用において参照されることにより、ネットワークカメラを始めとする IoT システムの情報セキュリティが少しでも向上することを期待します。

1 https://www.nisc.go.jp/active/general/ 「政府機関等の情報セキュリティ対策のための統一基準群」参照

2 本書は調達者が本書の目的を理解した上で調達仕様書に転記し易い形で作成しています。設計構築を発注する業者向けに適したチェックリスト部分のみを抜き出した表も公開しています（4.1 節参照）。

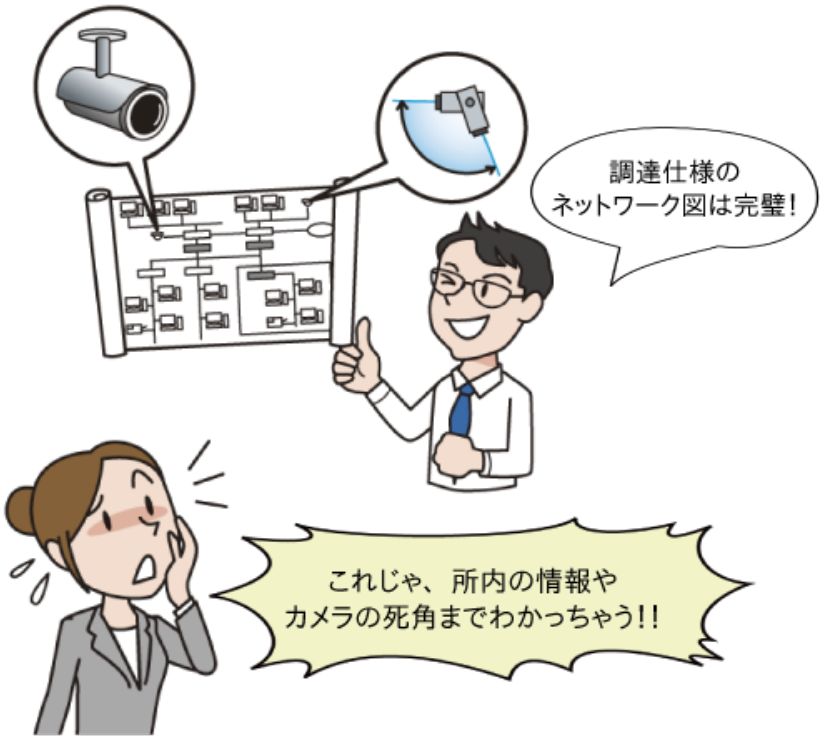
2. ネットワークカメラシステムのセキュリティ

この章では、チェックリストの必要性を理解するために、ネットワークカメラシステムが直面している特徴的な問題を紹介します。既に対策する必要に迫られていて、すぐにチェックリストを利用したい方は 3 章に進んでください。

2.1. 調達仕様策定において注意すべき事項

「4 チェックリスト」ではネットワークカメラを始めとする IoT システムにおいてマルウェアや攻撃者の侵入による、情報漏えいや改ざんといった脅威（「5.1 想定する脅威について」を参照）を想定し、それらに対策したシステムを構築、運用するための要件を記載しています。しかし、ビル監視を目的とするようなネットワークカメラシステムでは、構築されたシステムからだけではなく、設計構築を依頼するために作成した調達仕様の記載内容から攻撃のヒントとなる情報が漏えいする場合があります。

例： 調達仕様で公開する情報の吟味



ネットワークカメラシステムでは、建屋のレイアウトやネットワーク構成、IP アドレスの他、**カメラの位置**やカメラの**画角・稼働時間**など、セキュリティ上外部に公開して大丈夫な情報であるかを吟味して調達仕様を作成してください。情報の公開が必要な場合には、応札者に所定の場所で情報を参照してもらう等の対策が必要です。上記の他にも、機器名に部署名や場所を付けた場合、その情報から所内の機器のレイアウトが推測されてしまうこともあります。

2.2. システムの設計構築において注意すべき事項

ネットワークカメラシステムは、設計構築時に注意しなければならない情報セキュリティ上の事項があります。詳しくは「4.2 設計構築フェーズ」を参照して、調達仕様に転記してください。

例：　購入時のままのパスワード設定

管理機能などを用いる場合、通常パスワードが要求されます。このパスワードが製品出荷時に設定された値になっていると、製品マニュアルの情報を入手できるすべての人がそのシステムの管理者パスワードを知っていることとなります。パスワードは、システムを導入する組織の**情報セキュリティ対策基準や実施手順**[3]にのっとった値に必ず変更して運用しなければなりません。[a03-3]

また、ネットワークカメラは購入して繋ぐだけで利用できるようになる便利なサービスも動いています。不要なサービスは設計構築時に停止しましょう。[a02-1]

例：　購入時のままのファームウェアやソフトウェアでの運用

管理機能を使うためのパスワードは、調達者が意識して変更することができますが、IoT には、調達者が停止したりパスワードを変更したりできないバックドアと言われる侵入口が存在する場合があります。バックドアが発見されると、それを塞いだ新しいファームウェアが機器の提供元から公開されます。そのため、設計構築のタイミングでシステムを構成する機器が最新のファームウェアかどうかを確認し、必要に応じてバージョンアップを行うことが重要です。[a05-1] [g04-1]

管理機能上でのバージョンアップ操作が解りやすく、間違って不正なファームウェアが入らないように工夫された機器を選ぶことも重要です。

---

[3] 組織のセキュリティポリシーの下位文書（https://www.ipa.go.jp/security/manager/protect/pdca/policy.html 参照）

2.3. システム運用時に注意すべき事項

ネットワークカメラシステムでは、構築後の運用においても、保守やインシデントへの対応が必要となることがあります。詳しくは、「4.3 運用フェーズ」を参照してください。

例： 保守や障害への対応準備

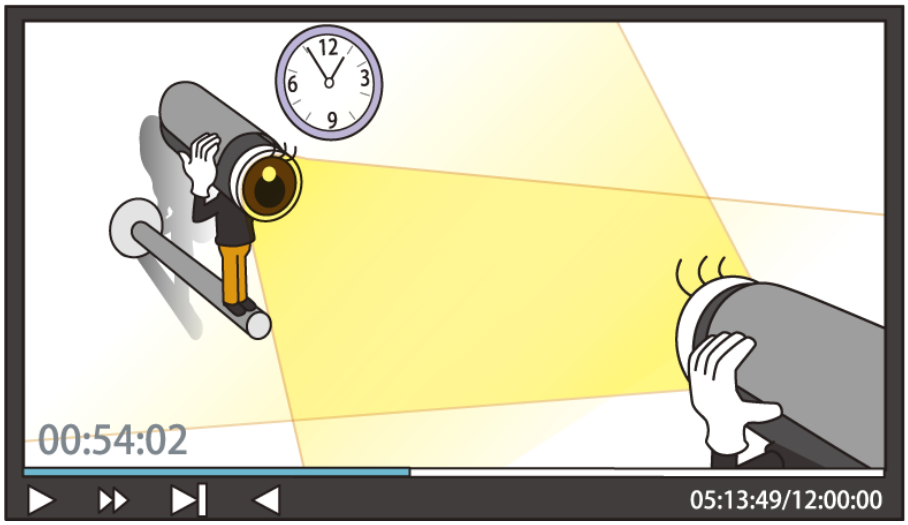
例えば、ネットワークカメラシステムで 24 時間監視を行っている場合、保守作業や障害が発生した際の一時的な停止や再起動に関しても、事前にセキュアな手順や保守計画を策定しておく必要があります。保守作業は、前項で紹介したような新たなバージョンのファームウェアが公開されたタイミングで突然発生することもあります。その時になって慌てないように、バージョンアップするかどうかを決定できるような適用基準と検討体制をあらかじめ決めておき、組織の**情報セキュリティ対策基準や実施手順**に規定しておくことが重要です。[f01-1][g05-1]

カメラ同士でお互いの画角を補い合うことにより、カメラ単位の停止が可能となるかもしれません。

例： 映像自体によるシステムのセキュリティの確保

本チェックリストでは正しい時刻設定が維持されることを要件としています。例えば監視カメラのシステムであれば、証拠として使われる可能性のある映像データやアラームに紐づけられる正確な時刻の維持が重要となります。システム内の各機器の時刻同期は一般的に NTP(ネットワーク・タイム・プロトコル)などを用いて行われますが、その情報がいつも信頼できるとは限りません。定期的に不自然な時刻の変化が無いことを確認することが重要です。 [a04-4] [g03-1]

物理的な時計や時報を、記録している画角内に設置するといった手法も対策の一つです。



2.4. システムの廃棄時に注意すべき事項

ネットワークカメラシステムは、その役目を終えてシステムを構成していた機器を廃棄する際にも、情報セキュリティの観点で考慮しなければならない事項があります。詳しくは「4.5 廃棄フェーズ」を参照してください。

例： 廃棄後のレコーダー等からの情報漏洩

機器の管理機能からデータ消去を実行しても、そのデータは復元可能な状態で機器内に残っています。レコーダーに残った映像情報など、漏えいすると問題となる情報が保存されていた機器に関しては、リース、レンタルの返却や廃棄処理を外部委託する際の処置について調達仕様で要件化（再生不能な電磁的フォーマットや物理的破壊を行い、消去証明書を提出するなどと記載）しておくべきです。[i01-1]

そのためには、あらかじめシステム内のどの機器に漏えいしては困る情報が保存されるのかを確認し、廃棄処理の対象とする機器をリストアップしておく必要があります。

3. チェックリストについて

本チェックリストはフェーズ（設計構築時、運用時、保守時、及び廃棄時）単位で節を分けて記載しています。ネットワークカメラシステム（以下、NWC システム）を調達する際は委託する事業範囲に合わせて、チェックリストの内容を仕様書に書き写してください。本チェックリスト中に記載している対策要件は、2018 年現在の一般的な IoT が持つ機能と、NWC システムに対する脅威[4]を考慮した最低限の情報セキュリティを担保するものです。機器やシステムの安全性や性能的要件、撮影した映像データの二次利用に伴うプライバシーの取扱いについては言及していません。

3.1. 対象とする利用形態

IP ネットワークで構築された NWC システム

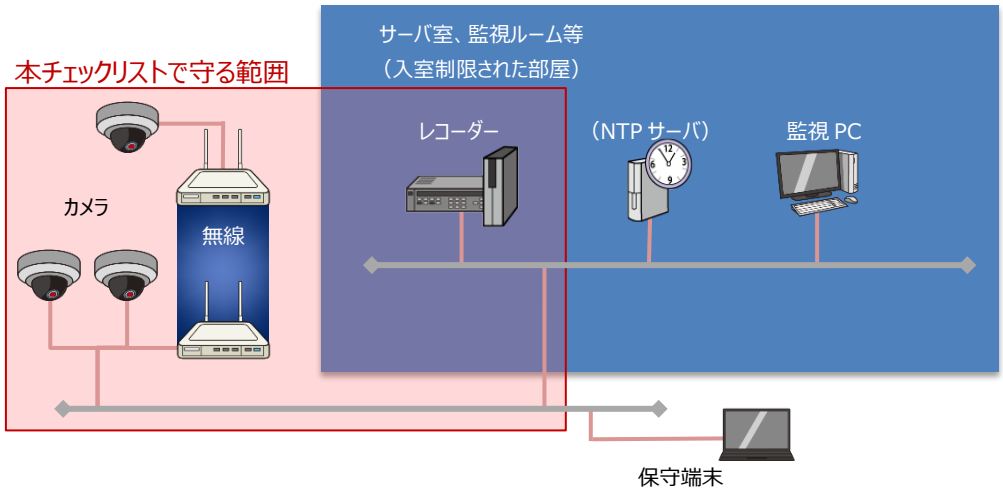


図 1　完全に独立した NWC システム

本チェックリストは IP ネットワークで構築された NWC システムを対象とします。ビル監視のような他のシステムから独立した IP ネットワーク上にカメラ、レコーダーが接続された NWC システム（図 1）、レコーダーが基幹ネットワークを介して他のシステムに接続された NWC システム（図 2）、及び河川監視などカメラが公共の場に設置され、カメラとレコーダー間の接続にインターネット回線を利用する NWC システム（図 3）を対象とします。[5]

これらの NWC システムでは、カメラを除く機器はサーバルームなど物理的な接触から保護された環境に置かれます。但し、カメラは人目にふれるところに設置されるため、カメラや、カメラに接続されるネット

[4] 本チェックリストで対策する脅威は「5.1 想定する脅威について」に例示しています。

[5] カメラをインターネットに接続する際は、その危険性について 3.4 節を参照してください。

ワーク回線は完全には保護されていない場合の追加要件を後述します。

また、2018 年現在の一般的な NWC システムの構築事例に従い、カメラはサーバとしてサービスを提供し、レコーダーはクライアントとして、カメラに映像データを取りにいく通信形態を対象とします（3.3 節参照）。

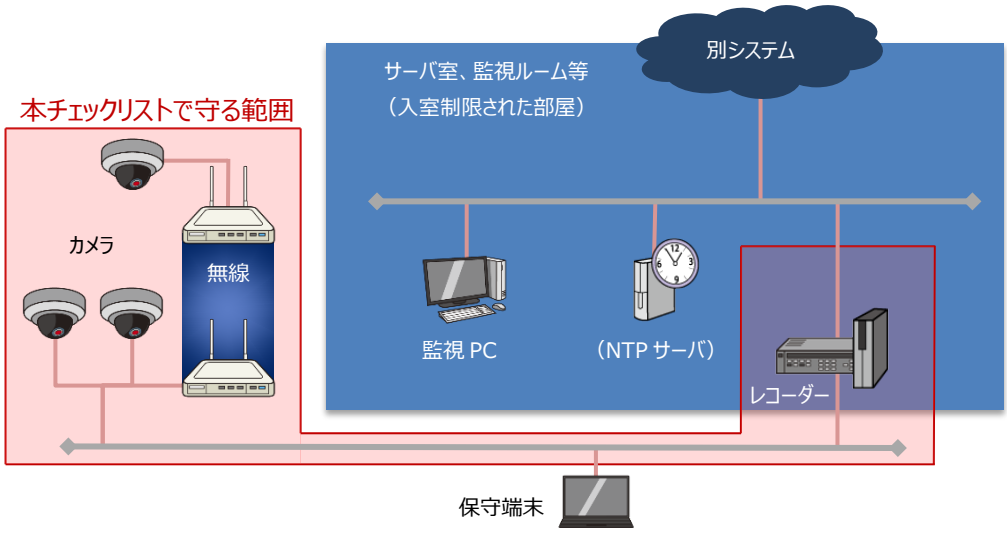


図 2　レコーダーが基幹ネットワークに接続されたシステム

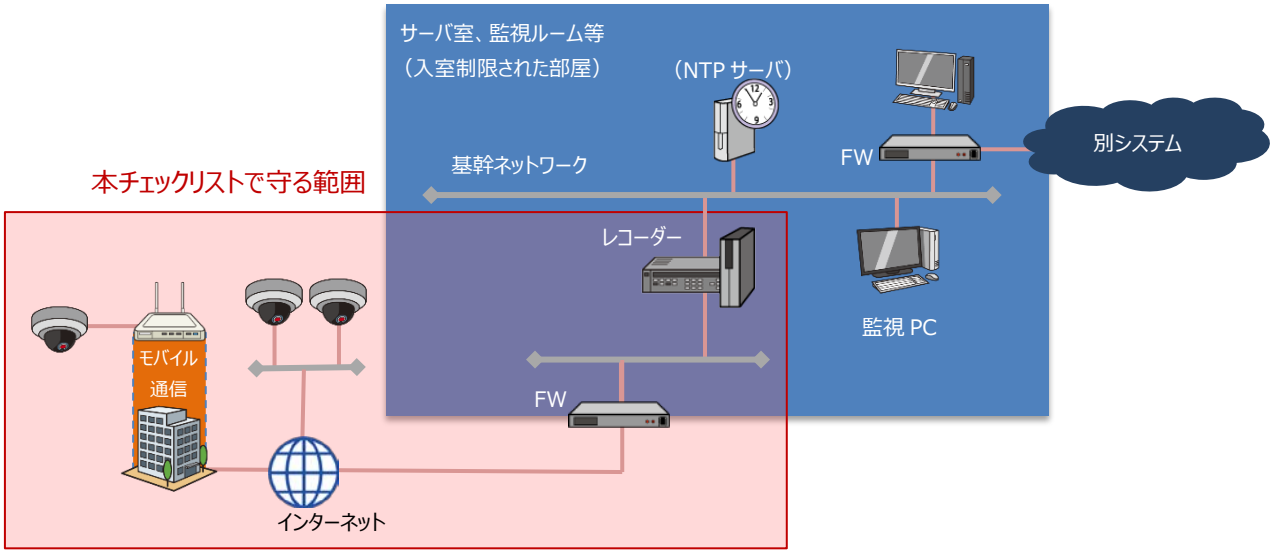


図 3　カメラとレコーダー間にインターネットを介す NWC システム

本チェックリストは、アナログカメラと同軸ケーブルで構成され、ビデオエンコーダーを介して IP ネットワークに接続された NWC システム (図 4)も対象とします。この構成はエレベーター内の監視目的などで現在も利用されています。

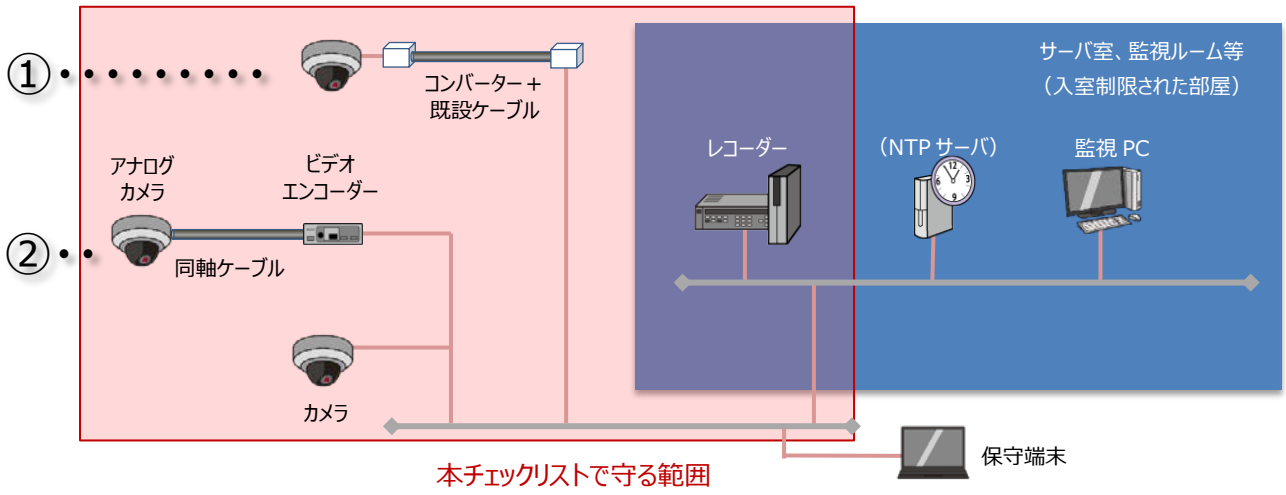


図 4　アナログカメラや同軸ケーブルを含む NWC システム

既設の同軸ケーブルを IP ネットワークの線として再利用している場合（図 4 の①）は、そのまま本チェックリストを適用します。アナログカメラが NWC システムに接続されている場合（図 4 の②）は、ビデオエンコーダーに対して本チェックリストのカメラに対する要件と同様の要件が必要です。4 章に記載されているビデオエンコーダーの機能要件を適用してください。アナログカメラへの要件はありません。

なお、本チェックリストでは、同軸ケーブルを流れるアナログ信号の盗聴やアナログカメラへのネットワークを介した攻撃は想定しません [6]。

6 一般的にアナログカメラはサーバ機能を持たず、また同軸ケーブルからの盗聴を気付かれずに行うことは困難なため、IP ネットワークと比較して攻撃を受ける機会が極めて低いためです。

3.2. 前提条件

本チェックリストでは、以下の役割を定義します。攻撃者として「第三者」と「利用者」を想定します。

役割		想定する攻撃機会
名称	説明	
第三者	NWC システム内のいずれの機器にも正当なアクセス権を所有しない者	機器への物理的な接触 （カメラ等の簡単に触ることができる機器への接触）
		ネットワークへの接続 （無線 LAN への接続、ネットワーク回線へのタッピングや露出している接続ポートへの接続）
利用者	管理者により NWC システムに対する一部のアクセス権を付与された者	アクセス権を越えた操作や閲覧 （管理者や保守員のみに許可された操作の実施）
管理者	利用者登録やログ監査等を行う NWC システムの運用管理者	本チェックリストでは攻撃者として考慮しない
保守員	ファームウェアのアップデート、アラームの受信を管理者に代行して請け負う者、SIer や保守業者	本チェックリストでは攻撃者として考慮しない

また、便宜上 NWC システムに存在する各種データを以下の通り分類します。

データ		具体例
名称	説明	
保護資産	録画（録音）されレコーダーに蓄積されたデータや NWC システム管理上のパスワードや証明書といった漏えいや改ざんが問題となるデータ	映像データ
		パスワード、サーバ証明書、暗号鍵
設定・制御データ	管理者や保守員が機器に設定するデータの中で漏えいした時点では問題とならないが、改ざんや再利用されると問題となる場合があるデータ	暗号化の種類、アラームの設定、ログ、ログの設定、画質や音質の設定値 カメラのパン・チルト・ズーム、設定の動的な変更、機器のリブートなどのために生成・発信さる制御データ
その他	本チェックリストでは保護対象としないデータ。NWC システム外に送付される映像データ、ログデータ、アラームや NWC システムが独自に作成・使用するデータ。	

3.3. カメラとレコーダー間の通信について

カメラ[7]とレコーダーの間では図 5 に記載した保護資産が通信されます。ネットワーク回線やハブ（HUB）への物理的な接続などにより攻撃者はこの通信を盗聴できますが、攻撃が困難なため、現在は脅威として想定していない NWC システムも多く存在します。

管理者が通信路の盗聴を脅威として想定する場合は、流れるデータ全てを保護する必要があるのか、パスワードなどレコーダーからカメラに送られるデータを保護すれば良いのか（図 6）を明確にした上で、本チェックリストの「d.カメラとの通信が盗聴される脅威を想定した NWC システムの追加要件」を追加してください。なお、通信の暗号化を要件とした場合は、暗号処理に伴う性能的な制約からレコーダーが管理できるカメラの台数が減るなどの影響がでることに留意してください。

本チェックリストでは、カメラとレコーダー間に VPN 網ではないインターネット回線を利用する NWC システムのみ通信の暗号化を必須要件とします。

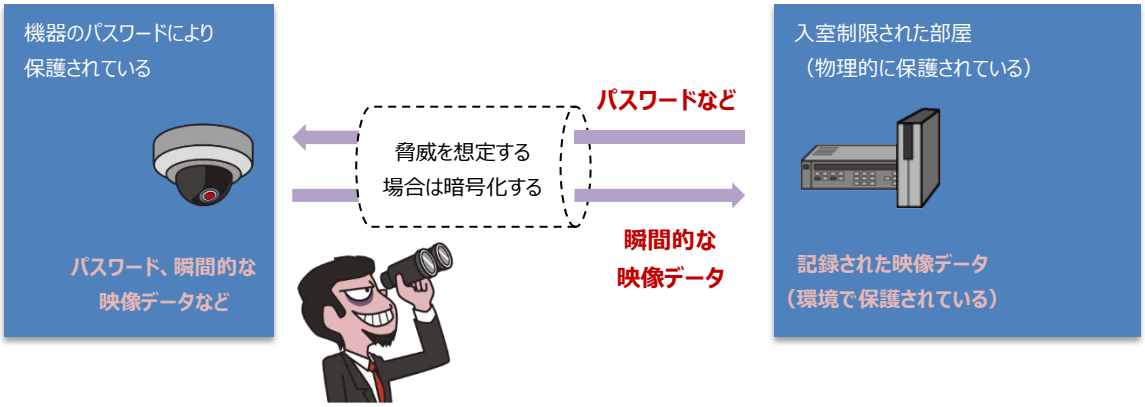


図 5　カメラとレコーダー間を流れるデータの例

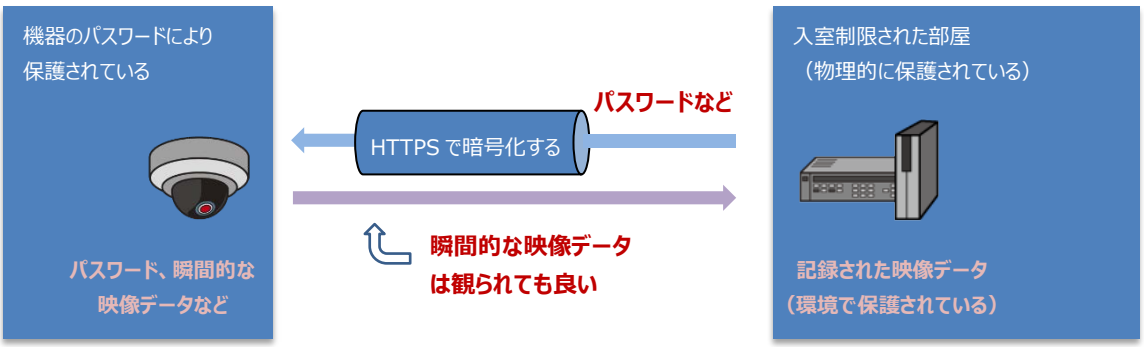


図 6　回線を流れる映像データまでは保護しない場合の例

[7] アナログカメラの場合はビデオエンコーダー

3.4. カメラをインターネットに接続する際のリスクと対策

カメラがインターネットに接続されていて不特定多数の人や機器からインターネット経由でのアクセスを許可している NWC システムでは、接続元の制限やセキュアなネットワークサービスの利用などによる対策が必要です。

インターネットからアクセス可能なカメラが受ける攻撃は、3.2.節で定義した第三者が行うカメラ-レコーダー間の回線へのタッピングや HUB への接続を前提とした攻撃と比較して、その種類が増えることはありません。しかし、攻撃者はより安全な場所から多くの時間と情報を使って効率的に攻撃できるため、以下の攻撃が現実的になります。2018 年現在、検索サービス[8]を用いて既知の脆弱性が存在するカメラを探し出すことは可能であり、その作業を代行するツールの存在も確認されています。

- **DDoS**
- **既知脆弱性やバックドアの利用**
- **識別認証機能への辞書攻撃／総当たり攻撃**

本チェックリストでは、インターネットからアクセス可能なカメラが受ける攻撃に対して「a.必須要件」、及び「d.カメラとの通信が盗聴される脅威を想定した NWC システムの追加要件」で対策していますが、長い時間や、新しい脆弱性を利用した攻撃を完全に防ぐことはできません。リスクをより軽減するために、VPN 網や、キャリアが提供しているセキュアな閉域網の利用を推奨します。

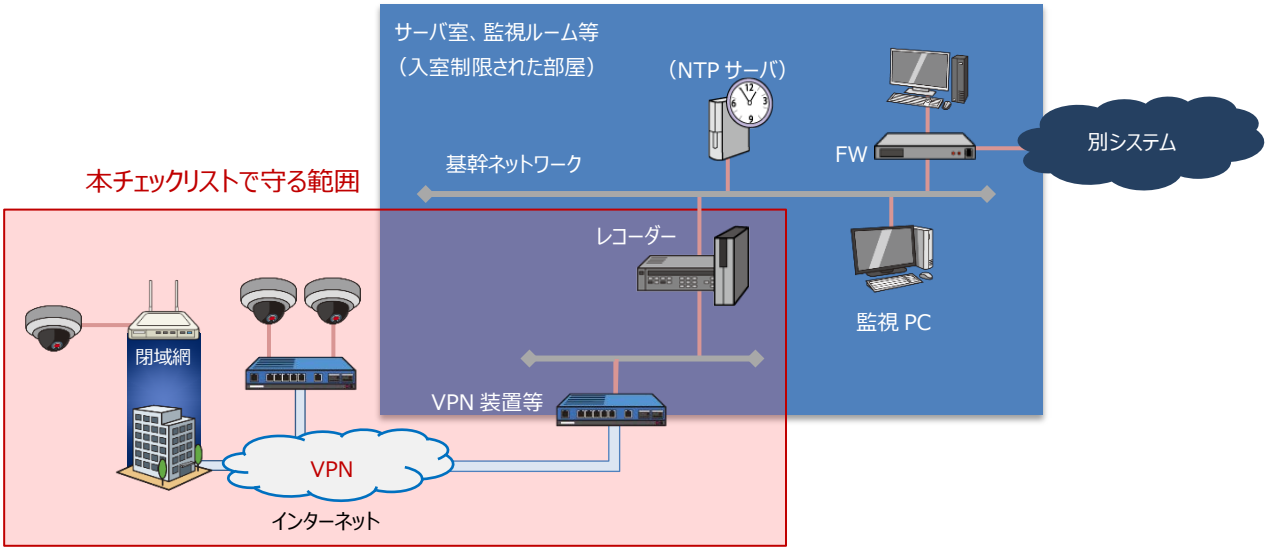


図 7　VPN 網により保護されたネットワーク構成の例

[8] SHODAN、insecam、censys、ZoomEye、SmartEye などインターネットからアクセス可能なカメラを検索し公開しているサービスが知られています。

4. チェックリスト

以下の対策要件のうち「必須要件」は、2018 年現在の IoT 機器が持つ機能及び導入事例を踏まえた最低限の要件です。基幹ネットワークに接続されている場合は「b.レコーダーがサービスを提供する場合の追加要件」、カメラへのいたずらや破壊行為を懸念する場合は「c. カメラへの物理的攻撃を想定した NWC システムの追加要件」、カメラとレコーダー間に VPN 網ではないインターネット回線を利用する場合、または NWC システム内においてネットワークの盗聴が懸念される場合は「d.カメラとの通信が盗聴される脅威を想定した NWC システムの追加要件」、そして無線 LAN による通信区間が存在する場合は「e.無線 LAN を用いている NWC システムの追加要件」をそれぞれ追加してください。

4.1. チェックリストの使い方（調達時の例）

チェックリストは、調達仕様に従ってシステムを構築するシステムインテグレーター（SIer）が参照する要件と、その要件を満たすために SIer が調達する各機器に求める機能性の要件を分けて記載しています。[9] 各機器が単体で機能性を満たせない場合は、他の機器やネットワーク構成で代替してください。

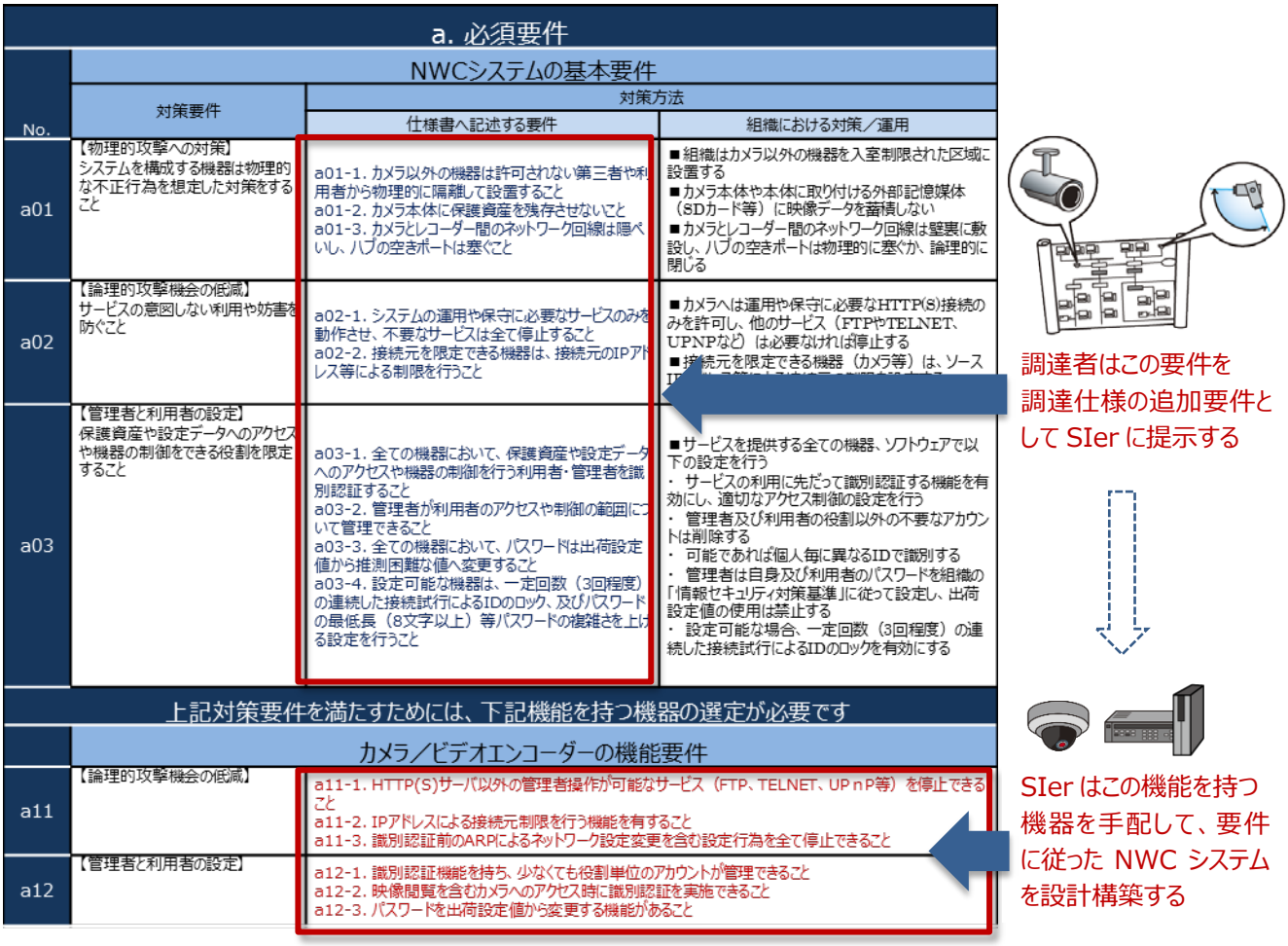


図 8　チェックリストの見方

[9] チェックリストを抜き出した編集可能なシートを以下からダウンロードできます。
https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/checklist_nwc.xlsx

4.2. 設計構築フェーズ

設計構築フェーズでは、管理者は以下のセキュリティ対策要件を満たすように、「仕様書へ記述する要件」に記載された事項を情報セキュリティに対する要件として仕様書に追記してください。設計構築の一部を組織が実施する場合は、「組織における対策／運用」を参照してください。

a. 必須要件			
No.	NWC システムの基本要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
a01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	a01-1. カメラ以外の機器は許可されない第三者や利用者から物理的に隔離して設置すること a01-2. カメラ本体に保護資産を残存させないこと a01-3. カメラとレコーダー間のネットワーク回線は隠ぺいし、ハブの空きポートは塞ぐこと	■組織はカメラ以外の機器を入室制限された区域に設置する ■カメラ本体や本体に取り付ける外部記憶媒体（SD カード等）に映像データを蓄積しない ■カメラとレコーダー間のネットワーク回線は壁裏に敷設し、ハブの空きポートは物理的に塞ぐか、論理的に閉じる
a02	【論理的攻撃機会の低減】 サービスの意図しない利用や妨害を防ぐこと	a02-1. システムの運用や保守に必要なサービスのみを動作させ、不要なサービスは全て停止すること a02-2. 接続元を限定できる機器は、接続元の IP アドレス等による制限を行うこと	■カメラへは運用や保守に必要な HTTP(S)接続のみを許可し、他のサービス（FTP や TELNET、UPNP など）は必要なければ停止する ■接続元を限定できる機器（カメラ等）は、ソース IP アドレス等による接続元の制限を設定する
a03	【管理者と利用者の設定】 保護資産や設定データへのアクセスや機器の制御をできる役割を限定すること	a03-1. 全ての機器において、保護資産や設定データへのアクセスや機器の制御を行う利用者・管理者を識別認証すること a03-2. 管理者が利用者のアクセスや制御の範囲について管理できること a03-3. 全ての機器において、パスワードは出荷設定値から推測困難な値へ変更すること a03-4. 設定可能な機器は、一定回数（3 回程度）の連続した接続試行による ID のロック、及びパスワードの最低長（8 文字以上）等パスワードの複雑さを上げる設定を行うこと	■サービスを提供する全ての機器、ソフトウェアで以下の設定を行う ・ サービスの利用に先だって識別認証する機能を有効にし、適切なアクセス制御の設定を行う ・ 管理者及び利用者の役割以外の不要なアカウントは削除する ・ 可能であれば個人毎に異なる ID で識別する ・ 管理者は自身及び利用者のパスワードを組織の「情報セキュリティ対策基準」に従って設定し、出荷設定値の使用は禁止する ・ 設定可能な場合、一定回数（3 回程度）の連続した接続試行による ID のロックを有効にする
a04	【不正アクセスの検知】 システムを構成する機器への不正アクセスやなりすましを検知すること	a04-1. システムがカメラやネットワークの切断（再接続）を検知できること a04-2. 連続したログインやシステムからの接続の失敗、及び／または管理者が覚えのない認証成功を検知し、確認する手段を管理者に提供すること a04-3. 映像データやログはその事象の発生時刻とともに記録すること a04-4. システムの時刻は正しく設定し、構築後に大幅な時刻データの変更が生じた場合は管理者が検知できること	■レコーダーのカメラの切断（再接続）検知機能を ON にする ■管理者はレコーダーのログ／アラームにおいて不正な識別認証の試行とみなすシステムからの接続を含むログインの連続試行、及び／または管理者が覚えのない接続やログイン成功を検知し通知される設定を行う。通知できない場合、管理者は定期的にログを確認する。 ■管理者はシステムの時刻を正しく設定し、維持する

a05	【既知脆弱性への対応】 システムを構成する機器は公知の脆弱性に対応済みであること	a05-1. システムを構成する全ての機器は、構築時点で公開されている脆弱性に対応したバージョンとすること	■システム稼働前に、ベンダサイト、及び公知脆弱性情報を、システムを構成する機器の製品名・型番等で検索し、該当する脆弱性があった場合は対策済みの最新のファームウェアにアップデートを行う
a06	【障害発生への対応】 障害の発生に対する対応が明確であること	a06-1. システムを構成する機器が無応答、もしくはサービス停止した時に、復旧（リブート）する手順を示すこと	■機器の障害発生時に再起動する手順を運用開始前に確認する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	カメラ／ビデオエンコーダーの機能要件		
a11	【論理的攻撃機会の低減】	a11-1. HTTP(S)サーバ以外の管理者操作が可能なサービス（FTP、TELNET、UPｎP 等）を停止できること a11-2. IP アドレスによる接続元制限を行う機能を有すること a11-3. 識別認証前の設定行為（ARP によるネットワーク設定変更を含む）を停止できること	
a12	【管理者と利用者の設定】	a12-1. 識別認証機能を持ち、少なくても役割単位のアカウントが管理できること a12-2. 映像閲覧を含むカメラへのアクセス時に識別認証を実施できること a12-3. パスワードを出荷設定値から変更する機能があること	
a13	【不正アクセスの検知】	a13-1. 認証成功の記録及び／または連続した認証失敗をログやアラームとして出力できること a13-2. ログは事象発生の時刻とともに記録できること	
a14	【既知脆弱性への対応】	a14-1. HTTP(S)経由でのバージョンアップ、及び動作しているファームウェアのバージョン確認ができること	
	レコーダーの機能要件		
a21	【不正アクセスの検知】	a21-1. カメラとの通信切断を検知する機能を持つこと	
a22	【既知脆弱性への対応】	a22-2. 機器の場合はバージョンアップ及び動作しているファームウェアのバージョン確認、ソフトウェアの場合はバージョンの確認が画面上でできること	
	ビデオエンコーダーの機能要件		
a31	【不正アクセスの検知】	a31-1. カメラからの信号消失を検知する機能を持つこと	

監査のポイント！

- 本システムのセキュリティに関する役割や手順が規定された文書は存在しますか？
- システムの受入れ時に仕様書で定められたセキュリティ要件が満たされていることを確認しましたか？
- システムを構成する機器やソフトウェアに既知の脆弱性が存在しないか確認していますか？
- システムを構成する機器やソフトウェアにセキュリティ侵害につながる重要な脆弱性が発見された場合、それを識別して修正が施せるようになっていますか？
- 管理者パスワードは出荷時のものや簡単に推定可能なものを設定していませんか？
- 時刻は正しく設定されていますか？

レコーダーが閉域網内の監視 PC や、基幹ネットワーク側へ映像閲覧などの Web サービスを提供する場合は、以下の要件を追加してください。前提として基幹ネットワークとカメラに接続されたネットワークは論理的に分離しており、IP ルーティングされないこととします。

b. レコーダーがサービスを提供する場合の追加要件			
	NWC システムへの追加要件		
No.	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
b01	【論理的攻撃機会の低減】 サーバサービスを提供する機器は接続元を制限すること	b01-1. レコーダーの基幹ネットワーク側からの通信は（HTTPS など）必要最低限のサービスのみとし、それ以外のサービスは全て停止すること	■レコーダーの基幹ネットワーク側からの通信は HTTPS 接続のみを許可し、他のサービス（FTP や TELNET、UPNP など）は明示的に停止すること
b02	【通信路の保護】 ネットワークを流れるデータを保護すること	b02-1. 基幹ネットワーク内で信頼できるサーバ証明書によりレコーダーを認証できる構成とすること	■可能な場合、基幹ネットワーク内で信頼する証明書を生成し、レコーダーのサーバ証明書として登録する
b03	【不正アクセスの検知】 システムを構成する機器への不正アクセスやなりすましを検知すること	b03-1. ログイン画面への連続した接続試行、及び／または管理者が覚えのないログインを検知し確認する手段を管理者に提供すること	■管理者はレコーダーのログ／アラームにおいて不正なログインとみなすログインの連続試行、及び／または管理者が覚えのないログイン成功を検知し通知される設定を行う。通知できない場合、管理者は定期的にログを確認する。
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	レコーダーの機能要件		
b21	【論理的攻撃機会の低減】	b21-1. HTTPS サーバ以外のサービス（HTTP、FTP、TELNET、UPnP 等）を停止できること b21-2. IP アドレスによる接続元制限を行う機能を有すること b21-3. 識別認証前の設定行為を停止できること	
b22	【役割単位の識別認証】	b22-1. 識別認証機能を持ち、少なくても役割単位のアカウントが管理できること。 b22-2. 映像閲覧を含むレコーダーへのアクセス時に識別認証を実施できること	
b23	【不正アクセスの検知】	b23-1. 連続したログイン試行及び／またはログイン記録をログやアラームとして出力できること	
b24	【通信路の保護】	b24-1. HTTPS サーバの機能を持ち、サーバ証明書をインストールする機能を持つこと b24-2. 平文で（暗号化せずに）送信されるログやアラームに保護資産を含まないこと	

監査のポイント！

- ネットワークにつながる機器において有効となっているサービスの必要性は把握していますか？　定期的に確認していますか？

必須要件では、カメラ機器自体への破壊行為への対策（抑止や検知）は行いません。設置場所等の環境によりカメラの破壊など物理的な攻撃が懸念される場合には、以下の要件も追加してください。但し、いたずらの検知機能の利用と耐衝撃性をもつカメラの導入では対象とする攻撃行為が異なります。[10]NWC システムの環境や予算に応じて、双方もしくは一方のみを追加要件としてください。

c．カメラへの物理的攻撃を想定した NWC システムの追加要件			
No.	NWC システムへの追加要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
c01	【物理的攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	c01-1．カメラへのいたずらを検知できるシステム設計を行なうこと c01-2．耐衝撃性をもつカメラを用いてシステムを構築すること	■管理者はカメラへの接触やいたずらを検知できるようカメラ、またはレコーダーを設定する ■耐衝撃性をもつカメラを選定し、ベンダ指定の方法にて設置する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	カメラ／ビデオエンコーダーへの追加機能要件		
c11	【物理的攻撃への対策】	c11-1．いたずらを検知する機能を持つこと（但し、レコーダーが当該機能を持つことを要件とした場合はカメラの要件とはしない） c11-2．カメラは 50J（IEC 60068-2-75／JIS C 60068-2-75）以上、または IK10（IEC 62262）以上に準拠していること	
	レコーダーの追加機能要件		
c21	【物理的攻撃への対策】	c21-1．いたずらを検知する機能を持つこと（但し、カメラ [11]が当該機能を持つ場合は要件とはしない）	

[10] 例えば、カメラを布で覆い隠す行為は、いたずらの検知により対策できますが耐衝撃性をもつカメラでは防止できません。一方でいたずらの検知機能により破壊行為の検知はできますが、破壊そのものを防ぐことができるのは耐衝撃性をもつカメラとなります。一般的に耐衝撃性をもつカメラはその分高価になります。

[11] アナログカメラの場合はビデオエンコーダー

カメラとレコーダー間に VPN 網ではないインターネット回線を利用するシステムは、以下の要件を必ず追加してください。

それ以外の場合であっても、カメラと他の機器との間のネットワーク回線やハブから通信が盗聴されることを脅威として考える場合は、対策として以下の要件も追加してください。対策は保護する対象とするデータで異なります。詳しくは「3.3 カメラとレコーダー間の通信について」を参照してください。

d. カメラとの通信が盗聴される脅威を想定した NWC システムの追加要件			
No.	NWC システムへの追加要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
d01	【通信路の保護】 ネットワークを流れるデータを保護すること	d01-1. カメラへの通信は HTTPS のみに限定すること d01-2. 必要な場合は、カメラからの映像データも HTTPS を使用すること d01-3. 可能な場合、システム内で信頼できるサーバ証明書によりカメラを認証できる構成とすること	■カメラは HTTPS の接続のみを許可する設定に変更する ■必要な場合は、レコーダー側で受け取るデータを over HTTPS に限定する ■可能な場合、システム内で信頼する証明書を生成し、カメラのサーバ証明書として登録する ■可能な場合、カメラの証明書のみを、クライアント（レコーダー）が信頼するように各クライアントを設定する
d02	【情報漏えい対策】 システムを構成する機器に関する不要な情報を漏らさないこと		■カメラの設定機能で設定可能な値に設置場所を特定できる名称を付けない（レコーダーや管理端末側でリンクさせるか、通信が保護されるオーバーレイ表示等を利用する）
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	カメラ／ビデオエンコーダーへの追加機能要件		
d11	【通信路の保護】	d11-1. HTTPS サーバの機能を持ち、サーバ証明書をインストールする機能を持つこと d11-2. 平文で（暗号化せずに）送信されるログやアラームに保護資産を含まないこと	

監査のポイント！

- HTTPS 接続で使用する暗号方式は電子政府推奨暗号リストに掲載されているような安全なものを使用していますか？

NWC システム内の機器間の通信の一部に無線を利用している場合は、以下の要件も追加してください。

e. 無線 LAN を用いている NWC システムの追加要件			
No.	NWC システムへの追加要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
e01	【無線通信路の保護】 無線 LAN 上のデータの盗聴・改ざんや無線ＬＡＮの不正利用を防ぐこと	e01-1. 無線 LAN の認証・暗号方式は WPA2-AES を使用すること e01-2. SSID は隠ぺいし、可能であれば接続元の MAC アドレス制限を行うこと e01-3. 無線通信 AP のパスワードは推測困難な値を設定すること	■無線 LAN の認証・暗号方式は WPA2-AES を設定する ■SSID は公開しない設定とし、システムの利便性に問題がなければ接続可能な機器を MAC アドレスにより制限する ■無線通信 AP のパスワードは推測困難な値を設定する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	カメラ／ビデオエンコーダー・レコーダーへの追加機能要件		
e11	【無線通信路の保護】	e11-1. 無線通信機能を有する場合には、WPA2-AES 方式をサポートすること。 e11-2. 無線通信 AP 機能を有する場合には、SSID の隠ぺい及び MAC アドレスによる接続制限ができること	

監査のポイント！

・　無線 LAN の認証・暗号方式は安全なものを使用していますか？　SSID は公開されていませんか？

NWC システムの可用性を要する場合は以下の要件を追加してください。可用性に関する要件は情報セキュリティの観点に限らず既に仕様書に記載されている場合がありますので、要件が重複しないように注意してください。

f. 可用性を要する場合の追加要件			
No.	NWC システムへの追加要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
f01	【可用性への対応】 システムが継続的に稼働できて、データ消失から免れること	f01-1. 保守作業のための機器単位の停止や、交換が可能なシステム設計を行なうこと f01-2. レコーダーに保存される映像データはミラーリング等によりデータ消失を防ぐ構成とし、障害時の復元手順を示すこと	■組織は保守のための定期的なシステムの計画停止、緊急時の一時的な停止を行う手順と判断基準を取り決める ■停止が不可能なシステムの場合は、カメラ映像の画角や機器の冗長構成を行い、機器単位の停止が可能な設計とする ■レコーダーのミラーリング等を行い、保存される映像データを冗長化する
上記対策要件を満たすためには、下記機能を持つ機器の選定が必要です			
	レコーダーの機能要件		
f21	【可用性への対応】	f21-1. ミラーリング等のデータ消失に備えた機能を有すること	

4.3. 運用フェーズ

NWC システムを導入した組織は、下表の「組織における対策／運用」を参照の上、組織の「情報セキュリティ対策基準」に伴うガイダンスや、組織のインシデント対応マニュアルに従い運用してください。運用業務を委託している場合は、組織における対策／運用の項目をそのまま運用の要件に加えてください。

g. NWC システム　運用フェーズ必須要件		
No.	NWC システムの基本要件	
	対策要件	対策方法
		組織における対策／運用
g01	【物理攻撃への対策】 システムを構成する機器は物理的な不正行為を想定した対策をすること	■(g01-1) アラーム（カメラの切断、映像の停止、カメラへの物理的攻撃を想定した場合は、いたずらの検知）に応じてインシデント対応を行う ■(g01-2) 定期的に機器に物理的な変化が無いかを確認するため、棚卸しを行う
g02	【管理者と利用者の設定】 保護資産や設定データへのアクセスを利用者のみに制限すること	■(g02-1) 機器やソフトウェアで設定したパスワードは、管理者や利用者の変更に伴い、組織の基準や方針に従って（削除、追加、変更など）運用する。必要な場合は利用者への指導を行う
g03	【不正アクセスの検知】 システムを構成する機器への不正アクセスやなりすましを検知すること	■(g03-1) 以下の事象を検知した場合、インシデント対応を行う ・ 連続したログイン試行、覚えのないログイン ・ 大幅な時刻の変更 ■(g03-2) 定期的にログを監査し、上記以外の不正なアクセスと考えられるログが無いことを確認する
g04	【既知脆弱性への対応】 システムを構成する機器は公知の脆弱性に対応済みであること	■(g04-1) 定期的にベンダサイト、及び公知脆弱性情報を、システムを構成する機器の製品名・型番等で検索し、該当する脆弱性があった場合は組織の基準や方針に従い脆弱性対応済のソフトウェアへの更新の要否を判断して（計画停止時などに）対応する
g05	【可用性への対応】 システムが継続的に稼働でき、データ消失から免れること	■(g05-1) 計画停止、及び保守作業を要すると判断した場合は、実施する日時を決めて保守フェーズを実施する ■(g05-2) アラームや管理者の操作によりカメラなどの機器のサービス停止を検出した場合で、g01【物理攻撃への対策】または g03【不正アクセスの検知】に該当しない場合は、障害発生時の手順に従って機器の再起動を行う ・「f.可用性を要する場合の追加要件」の対象機器は、その復元手順に従う

監査のポイント！

- システムの運用手順書は整備されていますか？　運用業務を委託している場合、セキュリティ対策が適切に運用されていることを確認していますか？
- データの定期的なバックアップはされていますか？
- 定期的なログの確認はなされていますか？
- 定期的な公知脆弱性情報の確認はなされていますか？
- インシデントが発生した場合の、対応手順を定めていますか？　インシデントの記録が残っていますか？

4.4. 保守フェーズ

管理者は、NWC システムの運用を委託する場合は「仕様書へ記述する要件」の要件を仕様書に追記してください。

h. NWC システム　保守フェーズ必須要件			
No.	運用フェーズへの移行に必要な要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
h01	【安全な再稼働】 保守後のシステムは設計された機能が再現できていること	h01-1. 保守フェーズ完了後に、追加（交換）された機器やソフトウェアが更新された製品が設計・構築フェーズの要件通りに設定され接続されたことを確認し、管理者に報告すること	■管理者は保守フェーズの前後で、稼働しているサービスや識別認証情報に相違が無いことを確認し、不備があれば設計構築フェーズに従い設定する（可能な場合はフェーズ前の状態への復旧も検討する）

監査のポイント！

- 保守作業の記録を残していますか？

4.5. 廃棄フェーズ

管理者は、NWC システムの運用を委託する場合は「仕様書へ記述する要件」の要件を仕様書に追記してください。

i. NWC システム　廃棄フェーズ必須要件			
No.	運用フェーズへの移行に必要な要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
i01	【安全なデータの廃棄】 廃棄された機器から保護資産が漏えいしないこと	i01-1. リースやレンタルから返却される機器や廃棄する機器に格納されたデータを再現不可能な方法で消去し、かつデータ消去の証明書を発行すること	■管理者はリースやレンタルから返却時または廃棄時、機器に格納された保護資産（必要な場合は設定データも）を論理的に消去すること ■組織はリース返却した機器の保護資産が全て安全に廃棄されたことをデータ消去証明書にて確認する

監査のポイント！

- リースやレンタルからの返却時あるいは廃棄時のデータ処理手順が存在し、実施記録がありますか？

5. 付録

5.1. 想定する脅威について

本チェックリストにおいて対策を講じた NWC システムの主な脅威は以下となります。

・機器への不正アクセスやマルウェア感染（ボット化）

第三者によるシステムへの不正アクセスやネットワークカメラへ影響を及ぼすマルウェアは、ネットワーク経由でアクセス可能な TELNET（TCP/23）や、UPnP（TCP/81）への通信と、管理機能への識別認証情報の設定不備 [12]や機器固有の脆弱性 [13]を利用して攻撃を試みます。それらは、機器の不要なサービスの停止と適切な識別認証情報の設定を行うことにより攻撃機会を大幅に低減することができます。本チェックリストでは【必須要件】[a02,a03,a05]にて対応します。

・管理者へのなりすまし

利用者による管理者への昇格も不正アクセスと同様に、管理機能への識別認証の不備や機器の脆弱性に起因します。【必須要件】[a03,a05]にて対応します。

・通信データの盗聴や改ざん

NWC システムでは、カメラやカメラが接続されているハブが第三者でも触れる場所に設置される場合があります。そこから通信内容を盗聴されると、映像データやパスワードなどの情報が漏えいしてしまいます。通信路上の盗聴や改ざんを脅威として想定する場合は【カメラとの通信が盗聴される脅威を想定した NWC システムの追加要件】[d01]を追記することにより対応します。NWC システム内の一部で無線 LAN を使用している場合は、無線 LAN をネットワークへの侵入口として悪用される可能性があるため、【無線 LAN を用いている NWC システムの追加要件】[e01]を追記して対応します。

・サービスや機器の停止

物理的なカメラの破壊や持ち去り、露出したネットワーク回線の切断は完全には防ぐことはできません。本チェックリストでは【必須要件】[a04]、及び【カメラへの物理的攻撃を想定した NWC システムの追加要件】[c01]によってその攻撃の検知と、ある程度の低減により対応します。なお、不特定多数に画像閲覧のサービスを提供するような NWC システムでは、そのサービスに対する DDoS による影響を防ぐことは困難です。できるだけ【必須要件】[a02]により、接続元を限定してください。

本チェックリストは、近年話題となっている IoT やネットワークカメラを標的としたマルウェアへの感染（ボット化）や、実際にインシデント事例が報告されているネットワークカメラへの侵入に対策することを目的として、市販の機器が実装している機能を適切に設定し、運用することを要件としています。長い時間を要するような高度な攻撃への対策は含めていません。IoT 製品は暗号化されたプロトコルを利用するだけでも処理性能に制限が出るため、閉域網の場合は、本当に脅威として想定するべきかを確認の上、必要な場合はその要件を仕様書へ追記するといった判断が大切です。

---

[12] 工場出荷時のデフォルトパスワードや簡単に推測できるパスワード

[13] 公知脆弱性として報告されるバックドアや、Web コンテンツに存在するコマンドインジェクションなど

5.2. 用語集

本チェックリスト内で使用している主な用語を解説します。

DDoS ： 複数の送信元から多量の処理を送りつけることによって、サービスを妨害することです

HTTPS ： 暗号化して Web ページの情報をやりとりするプロトコルです。ネットワークカメラでは設定変更や映像データの取得に利用します。システム内で対応している最新のバージョンと強固なアルゴリズムに限定します

MAC アドレス ： ネットワークインタフェース単位で持つ固有の値です。無線 LAN の接続元制限として補助的に利用される値ですが、詐称可能です

NTP サーバ ： 時刻を同期するためのサーバです。DDoS の送信元の一つとして利用されることがあります

SSID ： 無線のアクセスポイントを識別する値です。任意に設定することができるため、正しい SSID であれば正しいアクセスポイントであるとは言えません

UPnP ： 機器の検出などに使われるプロトコルです。悪用を避けるため、必要でない限り停止します

VPN ： 仮想的な閉域網です。本チェックリストでは VPN は閉域網と同等に扱います

VPN 装置 ： VPN を作成する機器です。上記の前提のために、装置は入室制限された部屋に設置され、インターネット側のネットワーク回線からの装置の管理はできないこととします

アクセス権 ： 識別認証された後の管理者や利用者に付与する権限です。識別認証される前は一般的に「ログイン画面」へのアクセス権しかありません

アラーム ： いたずらや不正アクセスを検知した際のメッセージです。管理者へのメール送信や画面上への表示など通知方法はシステムに合わせて設定します

暗号鍵 ： 暗号化されたデータを復号する際の計算に用いる値です

いたずらの検知 ： カメラの向きを変えたり、布を被せたりといったカメラへの物理的な不正行為を検知することです

映像データ ： カメラから出力されレコーダーに保存される画像や音声を含む映像のデータです

基幹ネットワーク ： 組織から許可された特定の第三者が組織の制限に従って接続しているネットワークです。そのため、組織内の第三者からの攻撃を受けます

サーバ証明書 ： HTTPS サーバには必ず存在する値で、暗号鍵とその持ち主の情報が含まれています。サーバ自体で作成することも、外で作成したものをインストールすることもできます。

サービス ： ネットワーク経由で提供するサーバ機能で、ポート番号（HTTP であれば 80 番、UPnP であれば 81 番など）を持ちます。不要なサービスは全て止めます

識別認証 ： 管理者や利用者の役割ごとに、本当にその人物かを、その人物しか知り得ない情報（ID とパスワードの組み合わせ）を用いて確認することです

耐衝撃性 ： 物理的な破壊行為に対して一定の基準を満たした耐性を持つことです。カタログでは耐衝撃型、バンダルプルーフ、またはバンダルレジスタントと書かれることもあります

ハブ（HUB） ： 複数のネットワーク回線を接続することにより、お互いの通信を可能とする機器です

パン・チルト・ズーム ： ネットワークカメラを左右・上下に動かすこと、及ぶ画角を拡大縮小することです。不正に動かされると、監視したい対象が映せなくなるといった問題が起こるため、制御する権限は制限するべきです

レコーダー ： 映像データを記録する機器やソフトウェアです。一般的に各カメラのスケジューリングや設定を行う管理ソフトの機能と、記録した映像を提供する機能を持ちます。記録した膨大なデータをバッチ処理でバックアップすることは困難なため、記録する映像データの可用性を考える場合は記録する段階でミラーリングなどを行います

ログ ： ログインに失敗した際や時刻を同期した際に残る記録です。この記録を元にアラームを送る設定をします

著作・制作	独立行政法人情報処理推進機構（IPA）
編集責任	山里 拓己
イラスト制作	株式会社 創樹
執筆協力者	特定用途機器情報セキュリティ対策検討委員会 手塚 悟　大久保 隆夫　吉岡 克成 根本 直樹　福田 次郎　荘司 憲男 羽部 高志　野口 英男 内閣官房 内閣サイバーセキュリティセンター 総務省 情報流通行政局 サイバーセキュリティ課 経済産業省 商務情報政策局 サイバーセキュリティ課 横浜市
IPA 執筆者	飛田 孝幸　井上 敬子

ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト

2018年3月30日　第２版発行

[事務局・発行]　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目28番8号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/security/jisec/choutatsu/


セキュアな
製品調達のために