攻撃カードと対応する対策一覧

	カード内容				対策及び対応するCSC番号（CIS Attackモデル，ATT&CK及びCAPEC参照）	
	No.	（PT）	タイトル	本文	対策	CSC番号
			Type A		攻撃カードType AはCSC開発時，対策の有効性を網羅的に確認する際に使用された抽象的な攻撃内容です．このため，対応する防御カードはType Bに比べ，多くなっています．	
1	No.1	（-3）		未保護の新規システムを継続的にスキャンし，脆弱性を悪用	脆弱性スキャンを実施可能な環境を見直す必要があります．脆弱性スキャンは専用のデバイスまたはソフトウェアにより実行させる可能性があります．このため，デバイス及びソフトウェアの適正な資産管理を実施し，不正なデバイス，ソフトウェアを検出する必要があります．ソフトウェアの完全性チェックによりソフトウェアの脆弱なバージョンを発見できる可能性があります．	**1(関連大)** 2.1-2.2 2.4-2.7 （特定）
					脆弱性スキャンにより，OS，ソフトウェア等の脆弱性なバージョンが暴かれる恐れがあります．同様にOS,ソフトウェア等の脆弱な設定も暴かれる恐れがあります．定期的にバージョンや設定を確認し，修正することで悪用のリスクを低減できます．リモート管理にはセキュアなチャネルを介することで悪用を防ぎます．重要システムファイルの変更を確認することで，悪用された可能性を確認できる可能性があります．	3 5 （防御）
					脆弱性スキャンにより弱いパスワードやデフォルトパスワードが特定される場合があります．管理者権限アカウントの認証情報が特定された場合，多大な損害を与える恐れがあります．このため，認証情報を含む管理者権限アクセスの適切なコントロールが望まれます．不正な管理者権限の使用にも気づけるようにすべきです．	4 （防御） （検出）
					システムが脆弱性スキャンされた場合，ネットワーク及びOS上に通常使用時とは異なる大量で不自然なログが出力されます．このため，適切な監査ログの保守，監視，分析の実施が望まれます．	2.3 6 （検出）
					ネットワークスキャンでは特定が難しいソフトウェアの脆弱性であっても，ホスト型のスキャナの使用や漏洩した管理者権限によるネットワークスキャンの使用から脆弱性が暴かれる可能性があります．電子メール及びWebブラウザクライアントの脆弱性の修正や対策が望まれます．	7.1-7.3 7.9-7.10
					ネットワークスキャンでは特定が難しいソフトウェアの脆弱性であっても，ホスト型のスキャナの使用や漏洩した管理者権限によるネットワークスキャンの使用から脆弱性が暴かれる可能性があります．脆弱性を突くマルウェアの対策が必要です．	8
					外部デバイスの利用を制限することで，不正な脆弱性スキャナの接続を防ぎます．	8.4
					脆弱性スキャンにより，システムで利用可能なポート，プロトコル，サービスが暴かれます．特に業務では使用しないポート等を経由し，攻撃を受ける恐れがあるためサービス等の制限を適切に実施する必要があります．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器にも脆弱性が存在します．クライアント及びサーバと同様にセキュアな設定やファームウェアのバージョンアップによりリスクを低減できます．２要素認証や暗号化セッションにより，管理することで，認証情報を保護します．	11 （防御）
					脆弱性スキャンはインターネット等の外部ネットワークから実施される場合があります．このため，内部システムとの境界上にセキュリティ装置を配置し，不審な通信を監視，防御する必要性があります．また，リモートログインアクセスを2要素認証とすることで，認証情報を保護します．	12 （防御） （検出）
					無線LANの脆弱性スキャンが実施される場合があります．例えば，暗号化通信の脆弱性を突かれ，通信内容を傍受される恐れがあるため，適切な管理が望まれます．	15 （防御）
					ネットワークスキャンでは特定が難しいソフトウェアの脆弱性であっても，ホスト型のスキャナの使用や漏洩した管理者権限によるネットワークスキャンの使用から脆弱性が暴かれる可能性があります．アカウント設定の脆弱性を悪用されるのを防ぎます．	16 （防御）
					Webアプリケーション等に対応した脆弱性スキャナは多数存在します．XSSやSQL等の不正な文字列を処理してしまうアプリケーションは攻撃者に悪用されます．このため，アプリケーションソフトウェアの適切な管理が望まれます．	18 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20 （復旧）
2	No.2	（-3）		パッチ処理が未完で，セキュリティ設定が不適切なクライアントソフトウェアの脆弱性を悪用	OS,ソフトウェア等のバージョン情報は資産管理ツールを利用することで特定できます．また，脆弱性が残るソフトウェアの使用制限や変更を検出できるようにします．OSログを取得することで不正な操作を発見できる可能性があります．	**2(関連大)** （防御）
					脆弱性スキャンにより，OS,ソフトウェア等のバージョンや脆弱な設定も明らかにできます．定期的にバージョンや設定を確認し，修正することで悪用のリスクを低減できます．リモート管理にはセキュアなチャネルを介することで悪用を防ぎます．重要システムファイルの変更を確認することで，悪用された可能性を確認できる可能性があります．	**5(関連大)** 3 （防御）
					設定の不備により弱いパスワードやデフォルトパスワードが悪用される場合があります．管理者権限アカウントの認証情報が特定された場合，多大な損害を与える恐れがあります．このため，認証情報を含む管理者権限アクセスの適切なコントロールが望まれます．不正な管理者権限の使用にも気づけるようにすべきです．	4 （防御） （検出）
					ソフトウェアの脆弱性を突く攻撃を実施した場合，ソフトウェアがクラッシュする場合があります．この場合，ログに記録されるため，監査ログの監視や分析が重要になります．	6 （検出）
					電子メール及びWebブラウザで利用するプラグインやスクリプトはよく悪用されます．不必要なスクリプトは無効化しておくことが望まれます．	7.1-7.3 7.9-7.10 （防御）
					マルウェアはMicrosoft，Adobe等のソフトウェアの脆弱性を悪用する場合があります．アンチウイルスソフトの他，EMET等の脆弱性緩和ツールを利用することでリスクを低減できます．外部デバイス経由による脆弱性の悪用を防ぎます．	8 （防御）
					端末上で起動する不要なサービスの悪用を防ぎます．	9.1-9.4

					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					クライアントPCに残置された不要なアカウントを悪用される場合があります．アカウントの有効期限の設定やスクリーンロックの設定等はOSのセキュリティ設定で実装されており，活用することが望まれます．不審なアクセス試行を検出できるようにします．	16 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					自社開発を含む全てのソフトウェアの脆弱性の悪用を防ぎます．	18.1-18.4 18.6-18.8 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
3	No.3	（-3）		継続的にソフトウェアをスキャンし，脆弱性を利用して対象マシンを侵害	脆弱性スキャンを実施可能な環境を見直す必要があります．脆弱性スキャンは専用のデバイスまたはソフトウェアにより実行させる可能性があります．このため，デバイス及びソフトウェアの適正な資産管理を実施し，不正なデバイス，ソフトウェアを検出する必要があります．ソフトウェアの完全性チェックによりソフトウェアの脆弱なバージョンを発見できる可能性があります．	1 **2(関連大)** （特定）
					脆弱性スキャンにより，OS，ソフトウェア等の脆弱性なバージョンが暴かれる恐れがあります．同様にOS,ソフトウェア等の脆弱な設定も暴かれる恐れがあります．定期的にバージョンや設定を確認し，修正することで悪用のリスクを低減できます．	5 **3(関連大)** （防御）
					システムが脆弱性スキャンされた場合，ネットワーク及びOS上に通常使用時とは異なる大量で不自然なログが出力されます．このため，適切な監査ログの保守，監視，分析の実施が望まれます．	6 （検出）
					ネットワークスキャンでは特定が難しいソフトウェアの脆弱性であっても，ホスト型のスキャナの使用や漏洩した管理者権限によるネットワークスキャンの使用から脆弱性が暴かれる可能性があります．電子メール及びWebブラウザクライアントソフトウェアの脆弱性の修正や対策が望まれます．	7.1-7.3 7.9-7.10 （防御）
					ネットワークスキャンでは特定が難しいソフトウェアの脆弱性であっても，ホスト型のスキャナの使用や漏洩した管理者権限によるネットワークスキャンの使用から脆弱性が暴かれる可能性があります．脆弱性を突くマルウェアの対策が必要です．外部デバイスの利用を制限することで，不正な脆弱性スキャナの接続を防ぎます．	8 （防御）
					脆弱性スキャンにより，システムで利用可能なポート，プロトコル，サービスが暴かれます．特に業務では使用しないポート等を経由し，攻撃を受ける恐れがあるためサービス等の制限を適切に実施する必要があります．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					脆弱性スキャンにより，システムで利用可能なポート，プロトコル，サービスが暴かれます．ネットワーク機器にトラフィック通過に関するセキュアな設定を施し，スキャンにより脆弱性が暴かれるリスクを低減します．	11.1-11.3 （防御）
					脆弱性スキャンはインターネット等の外部ネットワークから実施される場合があります．このため，内部システムとの境界上にセキュリティ装置を配置し，不審な通信を監視，防御する必要性があります．	12.1-12.10 （防御） （検出）
					Webアプリケーション等に対応した脆弱性スキャナは多数存在します．XSSやSQL等の不正な文字列を処理してしまうアプリケーションは攻撃者に悪用されます．このため，アプリケーションソフトウェアの適切な管理が望まれます．	18.1-18.8 18.10- 18.11 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
4	No.4	（-3）		マルウェア感染したマシンから他の脆弱なマシンを特定し，侵害	マルウェアの感染元は様々です．Conficker等の外部媒体を用いて感染拡大するマルウェアは多く存在します．無許可のデバイス接続が原因でネットワーク経由によるマルウェア感染のリスクも存在します．無許可なデバイスの接続の検出または制御することでリスクを低減できます．	1 （防御）
					実行ファイル型のマルウェアは無許可のソフトウェアと判断できます．ソフトウェアの棚卸しを適切に実施することで，リスクを低減できます．	**2(関連大)** （防御）
					マルウェアは感染したクライアントから他の脆弱性を悪用し，ネットワーク経由等で感染拡大が可能です．他のクライアントの脆弱性を残さないようにセキュアな設定や診断が望まれます．	3 5 （防御）
					マルウェアが起動すると通常とは異なるログを出力される場合があります．また，ネットワーク上にも特異な通信が発生する場合があります．このため，監査ログの適切な管理が望まれます．	6 （検出）
					マルウェアの感染元は様々です．電子メールまたはWebサイト経由で感染する場合があります．このため，電子メールとWebブラウザの適切な保護によりリスクを低減できます．	7 （防御）
					マルウェア感染にはアンチウイルスソフト等の一般的な対策が最も有効です．	8 （防御）
					ネットワーク感染型のマルウェアは様々なポート，プロトコル，サービスを悪用します．このため，不必要なサービスは排除しておく必要があります．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器にトラフィック通過に関するセキュアな設定を施し，感染マシンからの侵害へのリスクを低減します．	**11.1-11.3 (関連大)**

					マルウェアは感染後，C2サーバとアクセスし，遠隔操作により感染活動を展開する場合があります．外部システムとの境界上にセキュリティ対策を施すことで上記のリスクを低減できます．	12 （防御）
					マルウェアの感染元は様々です．無線LAN，Bluetoothや信頼できないデバイス経由でマルウェアの感染拡大する場合がある．このため，適切な無線アクセスコントロールの実施が望まれます．	15.1-15.6 15.8-15.10 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
5	No.5	（-3）		システムの脆弱なデフォルト設定を悪用	ハードウェア，ソフトウェアのデフォルト設定は脆弱な場合があります．社内のベースラインに基づき作成されたセキュアな設定をシステムに反映する必要があります．	**5(関連大)** （防御）
					システムの脆弱なデフォルト設定は脆弱性診断で発見することができます．	3 （防御）
					デバイスの管理権限アカウントには脆弱なデフォルトパスワードが存在します．管理者レベルの強固なパスワードに変更する必要があります．	4.2 4.4 （防御）
					マシンにプリインストールされたブラウザやメールクライアントのデフォルト設定により，マシンが侵害されるリスクがあります．セキュアな設定に変更する必要があります．	7.1-7.3 （防御）
					業務に不要なデフォルトの機能が動作している場合があります．セキュアな設定と比較する必要があります．	**11.1-3 (関連大)**
					無線アクセスポイントの脆弱性が悪用される可能性があります．無線LAN，Bluetoothや信頼できないデバイス経由でマルウェアの感染拡大する場合がある．このため，適切な無線アクセスコントロールの実施が望まれます．	15.6-15.9 （防御）
					ビルドインユーザやアカウント認証のデフォルト設定が悪用される場合があります．アカウントの有効期限の設定やスクリーンロックの設定等はOSのセキュリティ設定で実装されており，活用することが望まれます．	16.1-16.4 16.7-16.13 （防御）
					Webアプリケーションによっては不要な情報をエラーメッセージに表示してしまうものがあります．エラーメッセージの内容を修正し，悪用を防止します．	18.2 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9，19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
6	No.6	（-3）		継続的な脆弱性評価や修正が未実施のため，新たな重要パッチが未適用のシステムの脆弱性を悪用	無許可のデバイスは重要パッチが未適用の場合があります．無許可のデバイス経由によるシステムの侵害を防ぎます．	1
					無許可のソフトウェアが悪用される可能性があります．無許可なソフトウェアの脆弱性を悪用され，システムを侵害されるリスクを低減します．	2
					運用による設定変更，新規のパッチ未適用により新たに脆弱性が生起します．セキュアな設定の確認や脆弱性診断は定期的に実施することが重要です．	5 **3(関連大)** （防御）
					ソフトウェア等の脆弱性を悪用する場合，ソフトウェアがクラッシュする場合があります．この場合，不自然なログが出力されます．このため，適切な監査ログの保守，監視，分析の実施が望まれます．	6 （検出）
					Webブラウザ及びメールクライアントの脆弱性の悪用を防止するための対策が必要です．	7.1
					Microsoft，Adobe等のソフトウェアの脆弱性が悪用される場合があります．アンチウイルスソフトの他，EMET等の脆弱性緩和ツールを利用することでリスクを低減できます．	**8.1-8.3 (関連大)** （防御）
					サービス等がシステムの運用により追加される場合があります．このため，定期的にセキュアなベースラインとの比較を実施することは重要です．	9.2 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					運用によるネットワーク機器の設定変更，新規パッチの未適用のため，脆弱性が生起する場合があります．このため，定期的にネットワーク機器の設定を確認する必要があります．	11.1-11.3 （防御）
					インターネット等の外部ネットワークからサイバー攻撃を受ける場合があります．例えば，Webコンテンツを外部に公開している場合，コンテンツを更新することで脆弱性が生起する場合があります．このため，内部システムとの境界上にセキュリティ装置を配置し，不審な通信を監視，防御する必要性があります．	12 （防御） （検出）
					無許可の無線アクセスポイントの探索やセキュリティ設定の確認を継続して実施することでリスクを低減します．	15.1-15.3
					コンテンツの修正により，アプリケーションが新たにXSSやSQL等の不正な文字列を処理してしまう場合があります．また，最新パッチを未適用の場合があります．このため，定期的にアプリケーションソフトウェアを診断することが重要です．	18.1-18.8 18.10- 18.11 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9，19 （反応）

					定期的なペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
7	No.7	(-3)		対策の有効性測定や継続的改善が未実施の標的を攻撃	デバイス及びソフトウェアの棚卸し情報は変化します. 常時監視や検出により継続的な改善が可能になります.	1 2 (特定)
					運用による設定変更, 新規のパッチ未適用により新たに脆弱性が生起します. セキュアな設定の確認や脆弱性診断は定期的に実施することが重要です.	5 **3(関連大)** (防御)
					管理者権限の使用の適正性を確認できるプロセスを構築することで, リスクを低減します. 管理者権限使用の有効性を確認できるプロセスを構築します.	4.8-4.9
					ログに記録を残し, 確認することで対策の有効性を確認します.	6
					電子メールとWebクライアントによる対策を施し, 有効性を確認できるようなプロセスを構築します.	7.1 7.4 7.6
					継続的にマルウェア対策機能をモニタし, 有効性を確認します. DNSクエリをロギングし, 有効性を測定できるようにします.	**8.1-8.2** **8.6-8.8** **(関連大)**
					サービス等がシステムの運用により追加される場合があります. このため, 定期的にセキュアなベースラインとの比較を実施することは重要です.	**9(関連大)** (防御)
					攻撃が成功した場合, システムが汚染されます. 汚染されたシステムを完全に元の状態に修復することは非常に困難です. このため, 定期的にデータをバックアップすることで汚染前の状態に復元できるようにします.	10 (復旧)
					運用によるネットワーク機器の設定変更, 新規パッチの未適用のため, 脆弱性が生起する場合があります. このため, 定期的にネットワーク機器の設定を確認する必要があります.	11.1-11.4 (防御)
					インターネット等の外部ネットワークからサイバー攻撃を受ける場合があります. 例えば, Webコンテンツを外部に公開している場合, コンテンツを更新することで脆弱性が生起する場合があります. このため, 内部システムとの境界上にセキュリティ装置を配置し, 不審な通信を監視, 防御する必要性があります.	12.1-12.9 (防御) (検出)
					無線デバイスのセキュリティ設定を継続的に確認します. また, 不正な無線アクセスポイントを検知し, 改善を図ります.	15.1-15.3
					使用者の退職等で使用されなくなったアカウントが残置されている場合があります. このようなアカウントは悪用される場合があります. 定期的なアカウントの確認により, リスクを低減できます. AD等の集中型認証ポイントを使用することで, ログの確認を容易にします.	16.1-16.2 16.5-16.10 (防御)
					コンテンツの修正により, アプリケーションが新たにXSSやSQL等の不正な文字列を処理してしまう場合があります. また, 最新パッチを未適用の場合があります. このため, 定期的にアプリケーションソフトウェアを診断することが重要です.	18.3 18.7 (防御)
					攻撃が成功した場合, 迅速な対応が望まれます. 定期的なインシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります.	17.1-17.3 17.9, 19 (反応)
					定期的なペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	**20(関連大)** (復旧)
8	No.8	(-3)		悪意あるコードにより対象マシンを侵害し, 機密データを取得	悪意のあるコードは外部から持ち込まれたデバイス経由で実行される恐れがあります. 無許可なデバイスの接続の検出または制御することでリスクを低減できます.	1 (防御)
					実行ファイル型のマルウェアは無許可のソフトウェアと判断できます. ソフトウェアの棚卸しを適切に実施することで, リスクを低減できます. OSタイプに対応したイベントリツールによって, 悪意あるコードの実行を検出できる場合があります.	2 (防御)
					ソフトウェアの脆弱性を突くマルウェアが存在します. 定期的な診断により脆弱性を有するソフトウェアを検出し, 改善することで悪意のあるコードの実行を防止します.	3 (防御)
					悪意のあるコード実行時に様々なAPIが読み出されます. 見慣れないAPIの大量呼び出し等の異常なログにより, 悪意のあるコードの実行を検出できる場合があります.	6 (検出)
					悪意のあるコードは電子メールまたはWebサイト経由で実行される場合があります. このため, 電子メールとWebブラウザの適切な保護によりリスクを低減できます. 悪意のあるコードの侵入経路を塞ぎます.	7 (防御)
					悪意のあるコードの実行を防ぐにはアンチウイルスソフト等の一般的な対策が最も有効です. 外部媒体経由の侵害を防ぎます. C2サーバ経由の侵害を防ぎます.	**8(関連大)** (防御)
					攻撃が成功した場合, システムが汚染されます. 汚染されたシステムを完全に元の状態に修復することは非常に困難です. このため, 定期的にデータをバックアップすることで汚染前の状態に復元できるようにします.	10 (復旧)
					ネットワーク経由による不正なコードの実行を検出・防御します.	12.1-12.10 (防御)
					機密情報の漏洩を防止するため, 機密情報を特定し, 適切な管理を実施しておく必要があります.	**13(関連大)** (防御)
					Need-to-Knowの原則に従い, 機密情報とそれ以外の情報を適切にラベル付けし, 管理することでリスクを低減できます.	**14(関連大)** (防御)
					不正な無線アクセスポイントやBluetoothから悪意のあるコードの実行及び機密データの漏洩を防ぎます. BYODシステム等をネットワーク分割することでリスクを低減します.	15.2-15.6 15.9
					攻撃が成功した場合, 迅速な対応が望まれます. インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります.	17.1-17.3 17.9, 19 (反応)

					Webアプリケーション経由で悪意のあるコードを実行し，情報の取得される可能性があります．悪意のあるコードがWebアプリケーション上で実行されないようにすべきです．	18.1-18.4 18.6-18.8 18.10- 18.11
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
9	No.9	(-3)		業務に不必要なリモートアクセス可能なサービスを詳細にスキャンし，攻撃ルートを用意することでセキュリティを侵害	悪意のあるスキャンは外部から持ち込まれたデバイス経由で実行される恐れがあります．無許可なデバイスの接続の検出または制御することでリスクを低減できます．	1 （防御）
					無許可なソフトウェアの実行を検出，防止することで業務に不必要なリモートアクセス可能なサービスの起動を検出，防止することができます．	2 （防御）
					誤ったOSの設定により，不必要なリモートアクセス可能なサービス（例：Telnet）が起動しないようにセキュアな設定を施す必要があります．	5.1 5.2 5.4-5.5 （防御）
					定期的な脆弱性診断により，業務に不必要なリモートアクセス可能なサービスを検出することができます．	3.1-3.2 3.4-3.7 （防御）
					ネットワーク境界を監視し，不必要なリモートアクセス可能なサービスの利用を検出することができます．ログの適切な設定・確認が必要です．	6 （検出）
					マルウェアによってリモートアクセスサービスが悪用される可能性があります．マルウェア対策が有効です．外部媒体経由の侵害を防ぎます．C2サーバ経由の侵害を防ぎます．	**8(関連大)**
					起動中のサービス等が業務要件に即したもののみであることを確認し，不要なサービスを破棄することでリスクを低減できます．	**9(関連大)** （防御）
					トラフィックの通過を許可する設定を標準設定に追加する際は，変更内容を適切に把握できるように文書化し，業務に不必要なリモートアクセス可能なサービスを判別できるようにする必要があります．	**11(関連大)** （防御）
					ネットワーク境界のセキュリティ装置により業務に不必要なリモートアクセス可能なサービスへの詳細なスキャンを検知できます．	12 （防御）
					Need-to-Knowの原則に従い，機密情報とそれ以外の情報を適切にラベル付けし，管理することでリスクを低減できます．	14
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
10	No.10	(-3)		SQL インジェクション，クロスサイトスクリプティングなどにより脆弱なアプリケーションソフトウェアを悪用	バッファーオーバーフロー等により，アプリケーションがクラッシュした場合は，イベントログに保存され，検出できる可能性があります．	2.3
					脆弱性スキャンにより，OS，ソフトウェア等の脆弱性なバージョンが暴かれる恐れがあります．同様にOS,ソフトウェア等の脆弱な設定も暴かれる恐れがあります．定期的にバージョンや設定を確認し，修正することで悪用のリスクを低減できます．	3 5 （防御）
					ログを確認することで攻撃の成否を判定することができます．例えばSQLインジェクションの場合，不正な文字列を含む問い合わせの要求と応答結果から攻撃の成否を判別できます．このため，適切な監査ログの保守，監視，分析の実施が望まれます．	6 （検出）
					電子メール及びWebクライアントからスクリプトが実行されないための対策が必要です．	7 （防御）
					不正なスクリプトが実行されないようにマルウェア対策を施すことでリスクを低減できます．バッファーオーバーフローのようなソフトウェア脆弱性を突く攻撃のため，マルウェア対策が必要です．外部媒体からの混入を防御します．	8.1-8.5 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					SQLインジェクション等の攻撃は境界上にセキュリティ装置（IDS等）で検出，防御することができます．	12.1-12.7 （防御） （検出）
					Webアプリケーション等に対応した脆弱性スキャナは多数存在します．XSSやSQL等の不正な文字列を処理してしまうアプリケーションは攻撃者に悪用されます．このため，アプリケーションソフトウェアの適切な管理が望まれます．	**18(関連大)** （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	**20(関連大)** （復旧）
				無線アクセスポイントや無線クライアン	デバイスの資産インベントリを適切に管理することで，脆弱な無許可の無線アクセスポイント及びクライアントを検出することでリスクを低減できます．	1 （防御）
					無線アクセスポイントのリモート管理をセキュアなチャネルを介して実施することで悪用のリスクを低減します．無線アクセスポイントと無線クライアントの設定をセキュアな状態に保つことでリスクを低減します．	5.1-5.2 5.4-5.5 （防御）
					無線アクセスポイント及びクライアントへの継続的な脆弱性診断を実施することでリスクを低減することができます	3 （防御）
					無線アクセスポイントのログを取得し，分析することで異常な通信を特定できる可能性があります．	6 （検出）

11	No.11	(-3)		トやシステムの脆弱性を悪用し，内部ネットワークに侵入	攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					無線デバイスのセキュリティ設定及び使用する暗号化手法を堅牢な状態に保つ必要があります．	**15(関連大)** （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
12	No.12	(-3)		ソーシャルエンジニアリングによりユーザやシステム管理者を欺瞞	管理者の一部の認証情報が漏れた場合でも，多要素認証により，攻撃者の不正なアクセスを防御できる可能性があります．また，内部牽制機能や管理者権限の操作をログで監視することでリスクを低減することができます．	**4(関連大)** （防御） （検出）
					監査ログを収集し，管理者権限アクセスをモニターすることで不正な管理者権限の使用を検出できる可能性があります．	6
					電子メールによるなりすましはSPFで検出できます．不振なURLのアクセスを確認・防御します．	7.4-7.5 7.8 （防御）
					多要素認証により，一部の管理者認証情報が漏洩した場合のリスクを低減できます．	11.5 （防御）
					信頼できるサイトのみのアクセスを許可することで，不審なサイトへの誘導を防御します．2要素認証により認証情報の漏洩のリスクを低減します．	12.2-12.3 12.11
					Need-to-Knowの原則に従い，機密情報とそれ以外の情報を適切にラベル付けし，管理することで認証情報を取得された場合のリスクを低減できます．	14
					EAP/TLSを使用することでなりすましのリスクを低減できます．	15.8
					多要素認証により，一部の管理者認証情報が漏洩した場合のリスクを低減できます．不必要なアカウントの削除やスクリーンロック等により認証情報を適切に管理することで，認証情報の不正利用のリスクを低減できます．	**16.1-16.3 16.6-16.13 (関連大)** （防御）
					セキュリティスキル訓練を実施することでソーシャルエンジニアリングを見破れる可能性があります．	**17(関連大)** （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	19
13	No.13	(-3)		一時的に例外を認めたが修正されず，セキュリティ設定が脆弱なネットワークデバイスを悪用	一時的に例外を認められ，接続したデバイスを適切に管理し，修正することでリスクを低減します．	1
					定期的な構成設定を自動的に実施・再適用するシステム設定管理ツールを適用することで，例外の放置を修正できる可能性があります．	5.4 （防御）
					継続的な脆弱性診断により，修正されていないセキュリティ設定を検知できます．	3.1-3.2 3.4-3.6 （防御）
					適切にログを収集・分析することで攻撃内容を調査することができる可能性があります．	6
					定期的にポートスキャンを実施し，ベースラインと比較することで，未修正の例外を発見できる可能性があります．	9.3
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器のセキュアな設定と機器の設定を比較することで，変更を発見できる可能性があります．変更を実施した場合に文書に記録することで，管理が容易になり，修正のし忘れを防止できる可能性があります．	**11 (関連大)** （防御）
					ネットワーク機器の悪用からネットワーク機器を防御するため，境界防御によりリスクを低減できます．	**12 (関連大)**
					無線アクセスコントロールに関して，一時的に例外を認めた場合でも，セキュアな状態に修正することでリスクを低減します．	15
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーション時に作成したアカウントの除去を確認することで，悪用のリスクを低減できます．ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					実行ファイル型のマルウェアは無許可のソフトウェアと判断できます．ソフトウェアの棚卸しを適切に実施することで，悪意のあるコードが実行されるリスクを低減できます．	2 （防御）
					ソフトウェアの脆弱性を突くマルウェアが存在します．定期的な診断により脆弱性を有するソフトウェアを検出し，改善することで悪意のあるコードの実行を防止します．	3 （防御）
					管理権限を最小限に抑え，必要な場合にのみ管理アカウントを使用することで，プログラムを管理者権限で実行することが防ぐことができる可能性があります．管理者権限によるマシンの使用をモニタすることでリスク低減を図ります．	**4.3 4.8-4.9 (関連大)** （防御）
					悪意のあるコード実行時に様々なAPIが読み出されます．見慣れないAPIの大量呼び出し等の異常なログにより，悪意のあるコードの実行を検出できる場合があります．	6 （検出）

14	No.14	(-3)		フィッシングメールにより対象マシン上で悪意あるコードを管理者権限で実行	悪意のあるコードは電子メールクライアント機能の脆弱性を突く場合があります．このため，電子メールクライアント上の不要な機能を無効化することによりリスクを低減できます．悪意のあるコードの侵入のための入り口対策によりリスクを低減します．	7 （防御）
					悪意のあるコードの実行を防ぐにはアンチウイルスソフト等の一般的な対策が最も有効です．	8.1-8.3 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					悪意のあるコードが添付されたメールは境界ネットワークに配置されたセキュリティ装置により防御できる可能性があります．	12.1-12.3 12.6-12.7 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．また，フィッシングメールはトレーニングにより識別できる可能性があります．	**17(関連大)** 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
15	No.15	(-3)		インターネットからアクセス可能なDMZ上のシステム経由で内部ネットワークの深部まで侵入	外部に公開しているサーバのセキュリティ設定を堅牢な状態に保つ必要があります．このため，ハードウェア，ソフトウェアのセキュアな設定に係る項目を適切に実施しておく必要があります．	5.1-5.2 5.4-5.5 （防御）
					DMZ経由による内部システムへの侵入は公開サーバの脆弱性を利用される可能性があるため，継続的な脆弱性診断による改善はリスクを低減できます．	3 （防御）
					サーバ及びネットワーク境界デバイスのログを監視，分析することで，DMZ経由での攻撃を検出できる場合があります．	6 （検出）
					サーバが起動中のサービス等を悪用される恐れがあります．サービス等の制限，コントロールを適切に実施し，不要なアクセスを制限することでリスクを低減できます．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器のセキュアな設定を施し，不正アクセスのリスクを低減します．	11.1-11.3
					境界ネットワーク上のセキュリティデバイスにより，DMZ上のサーバへの攻撃やサーバを経由した攻撃通信を検知または防御できます．	**12(関連大)** （防御） （検出）
					Need-to-Knowの原則に従い，機密情報とそれ以外の情報を適切にラベル付けし，管理することで内部ネットワークの深部まで侵入されるリスクを低減できます．	14
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
16	No.16	(-3)		未保護の接続，脆弱なフィルタリング設定などの不適切なネットワークアーキテクチャの設定を悪用	デバイスの棚卸し管理を適切に実施することで，無許可のデバイスのネットワーク接続を検知，防御できます．	1 （防御）
					サーバ，ホスト，ネットワークデバイスなどのリモート管理はセキュアなチャネルを介して実施することで，盗聴されるリスクを低減できます．OS及びソフトウェアのセキュア設定を施し，定期的な確認によりネットワーク設定の脆弱性を低減します．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性診断により，脆弱なフィルタリング設定を発見できる可能性があります．	3.1-3.2 3.4-3.7 （防御）
					ネットワーク機器のログを監視，分析することで，不適切なネットワークアーキテクチャの設定を悪用する攻撃を検出できる場合があります．	6
					サービス等の制御において適切なフィルタリング設定の確認，検証を実施することで，リスクを低減できます．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器の設定について，適切に確認，検証を実施することで，リスクを低減できます．	11 （防御）
					境界ネットワーク上のセキュリティデバイスへのセキュアな接続を確保し，境界上を通過する通信をプロキシ経由にする等の境界防御によりリスクを低減できます．	**12(関連大)** （防御）
					Need-to-Knowの原則に従い，機密情報とそれ以外の情報を適切にラベル付けし，管理することでネットワーク設定の不備によるセキュリティ侵害を低減できます．	14
					無線アクセスにおいて，セキュアな設定の確認及び検証を実施することで，リスクを低減できます．	15 （防御）
					ネットワーク上でユーザ名と認証情報を送信する際，暗号化チャネルを利用することで，盗聴による認証情報の漏洩のリスクを低減できます．	16.5 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）
					自社開発のアプリケーションが適切に保護されていることを確認します．	18.9
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7

					DHCPサーバロギング機能を活用し，不明デバイスを検出します．	1.3
					使用中の各OSタイプに対応したソフトウェアインベントリツールを組織全体に適用し，ログを収集することでリスクを低減できます．	2.3 （検出）
					セキュアな設定により収集ログの選択やログの保存サイズ等を指定することができます．これにより，ログの収集漏れのリスクを低減できます．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性スキャンにより，ログ収集の設定漏れ等の不備を検出できる可能性があります．これにより，リスクを低減できる可能性があります．	3.1-3.2 （防御）
17	No.17	（-3）		ログ収集及びログレビューが未実施の標的システム上で，長時間，検知されることなく活動	ドメイン管理者グループへのアカウント追加・削除時や管理者アカウントへのログイン失敗時にログエントリを発行し，アラートを送信することで，管理者アカウントの悪用を早期に発見できる可能性があります．また，システムアクセス時に完全にログが記録される非管理者アカウントの使用を管理者に対し，義務付けることで管理者アカウントの使用者を特定できます．	4.8-4.9 （防御）
					サイバー攻撃を詳細に調査するため，ログの適切な管理が望まれます．監査ログの保守，監視，分析の各項目は適切なログ管理のためのプロセスです．	**6(関連大)** （検出）
					URLリクエストのログを収集することで，悪意のあるURLへのアクセスを特定できる可能性があります．	7.6 （検出）
					非公開データへのアクセスに関する詳細な監査ロギングを実装することで不審なアクセスを検出できる可能性があります．	14.9 （検出）
					監査ログによって存在しないアカウントへのアクセスの試行をモニタすることはログレビューの１つの方法です．	16.12- 16.13 （検出）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．ただし，不適切なログ管理はインシデント調査を困難にします．	17.1-17.3 17.9, 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					脆弱性スキャンの結果からリスク評価を実施し，適切な資産グループの基づくネットワーク分割を実施することで，機密文書漏洩のリスクを低減します．	3.8
					ファイルへのアクセスログを監視，分析することで，機密情報へのアクセスを検出できる場合があります．	6
					機密情報を格納するシステムで毎週より頻繁にバックアップを実施することで機密文書への改ざん，破壊から復旧できる可能性があります．	10.1 （防御）
					機密情報を特定し，認可されたハードドライブ暗号化ソフトウェアを適用したデバイスに保存することで機密データを保護することができます．	**13(関連大)** （防御）
18	No.18	（-3）		機密情報を適切に特定せず未保護な組織の機密文書にアクセス	Need-to-Knowによるアクセスコントロールを適切に実施することで，機密情報への不正なアクセスのリスクを低減できる可能性があります．	**14(関連大)** （防御）
					機密データへのアクセス権限があるすべてのユーザアカウントに多要素認証や長いパスワードを義務付けことで機密情報への不正なアクセスのリスクを低減できる可能性があります．アカウントの保護により，機密情報にアクセスされるリスクを低減します．	16 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17 19 （反応）
					監視下にない開発者が本番環境にアクセスし，機密情報を収集するリスクを低減します．自社開発のアプリケーションが適切に保護されていることを確認します．	18.9
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20 （防御）
					セキュリティ設定を適切に実施することでアカウントの有効期限等を設定でき，非アクティブアカウントを無効化できる可能性があります．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断によりセキュリティ設定を適切に実施し，アカウントの有効期限等のセキュアな設定を確認します．	3.1-3.2 3.4-3.7 （防御）
					多要素認証の仕組みを取り入れることで不正アクセスのリスクを低減します．	4.4
					アカウントの監査ログを監視，分析することで，非アクティブアカウントの悪用を検出できる場合があります．	6
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					２要素認証の仕組みを取り入れることで，不正アクセスのリスクを低減します．	11.5 12.11
19	No.19	（-3）		一時雇用者，請負業者，元従業員などが残した非アクティブアカウントを悪用	情報へのアクセスは業務に必要なものに限定し，定期的にアクセスしないものはネットワークから分離して保存することで，非アクティブアカウントの悪用のリスクを低減します．	14.1-14.3 14.5-14.7 14.9
					アカウントの監視，コントロールを適切に実施することで，非アクティブアカウントの悪用のリスクを低減できる可能性があります．	**16.1-16.3 16.5-16.10 16.12- 16.13 (関連大)** （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9, 19 （反応）

					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．また，ユーザアカウントなどがテスト終了後に除去されているか確認することが重要です．	20.1-20.3 20.5-20.7
20	No.20	(-3)		パスワード推測，パスワード解析，権限昇格の脆弱性を突く攻撃により管理者権限を取得し，他のマシンにも被害を拡大	マルウェアによる権限昇格のリスクを低減するため，無許可のソフトウェアの起動を制限するための対策が有効です．ソフトウェアイベントリツールを組織全体に適用します．	2.2 2.3 （防御）
					セキュリティ設定を適切に実施することでパスワードの複雑さやアカウントロック等が設定でき，パスワード推測攻撃のリスクを低減できます．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断によりセキュリティ設定が適切に実施し，パスワードの複雑さ等のセキュアな設定を確認します．	3 （防御）
					管理者権限の悪用を防ぐため，適切な管理者権限のコントロールされた使用に係る項目を実施する必要があります．	**4(関連大)** （防御）
					監査ログにより，ログインの連続失敗等の異常なログを確認することでパスワード推測攻撃等を発見できる可能性があります．	6 （検出）
					権限昇格の脆弱性を突くマルウェアのリスクを低減するため，アンチウイルスソフト等のマルウェア対策が有効です．	8.1-8.3 8.6 8.8 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワーク機器への認証に二要素認証を用いることで，パスワード推測のリスクを低減できます．管理用セグメントの利用により，物理的な対策により，リスクを低減します．	11.4 11.5 （防御）
					境界ネットワーク上にセキュリティ装置を配置することで公開サーバ等への権限昇格攻撃を検出・防御できる可能性があります．パスワード推測攻撃はIPSやIDSで検知・防御できます．	12 （防御）
					ネットワークを分割することで，侵入拡大のリスクを低減します．	14.1-14.3
					ログイン失敗回数に達した場合，アカウントが標準の期間，ロックされるように設定することでパスワード推測攻撃を低減できる可能性があります．機密データへのアクセス権限があるすべてのユーザアカウントに多要素認証や長いパスワード要求することで，パスワード推測のリスクを低減できます．全パスワードファイルが暗号化することで，パスワード解析のリスクを低減できます．	**16(関連大)** （防御）
					Webアプリケーション等の権限昇格の脆弱性に対する攻撃のリスクを低減するため，アプリケーションソフトウェアセキュリティの適切な管理が望まれます．	18.1-18.4 18.6-18.8 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
21	No.21	(-3)		システムの内部にアクセスし，検知されることなく機密情報を収集	デバイスまたはソフトウェアのインベントリを適切に作成しておくことで，不正なデバイス及びソフトウェアを検出することができます．	1 2 （特定）
					セキュアな設定により，ログ収集機能を有効化する設定とすることで，検知ができるようにします．	5.1-5.2 5.4-5.5 （防御）
					脆弱性を突き，内部に侵入されるのを防ぎます．	3.1-3.2 3.4-3.6
					管理者権限の不正利用を検知し，リスクを低減します．	4.8-4.9
					SIEMツールまたはログ分析ツールを適用し，監視することで不正アクセスを検出できる可能性があります．ログを適切に保守，監視，分析し，不正アクセスを検出できるようにします．	6 （検出）
					メール及びWeb経由で内部システムに侵入のためのマルウェアが送付される場合があります．不審メール，URLのフィルタリングを実施し，監視することでリスクを低減できます．	7 （検出）
					マルウェアを用いた内部システムへの侵入される場合があります．アンチウイルスソフトウェア等のマルウェア対策により検知できる可能性があります．C2サーバへの通信を防ぎます．外部媒体経由の感染を防ぎます．	8 （防御）
					許可された通信以外をドロップする拒否ルールを持つホストベースファイアウォールなどをホストに適用し，監視することでリスクを低減することができます．不要なサービス経由で内部システムにアクセスされるのを防ぎます．	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします．	10 （復旧）
					ネットワークの通信設定をセキュアにすることで，不正アクセスによる侵入のリスクを低減します．	11.1-11.3
					信頼できない外部システム経由で内部システムに侵入される場合があります．ネットワーク境界上にセキュリティ装置を配置し，通信情報を収集・監視することでリスクを低減することができます．	12 （防御）
					機密情報を特定し，暗号化や完全性コントロールを実施することで，リスクを低減することができます．	**13(関連大)** （防御）
					Need-to-Knowの原則に従い，機密情報とそれ以外の情報を適切にラベル付けし，管理することでネットワーク経由で機密情報を収集されるリスクを低減できます．	14 （防御）

					無線アクセスポイント経由で内部に侵入されるリスクを低減します.	15 （防御）
					監査ログによって存在しないアカウントへのアクセスの試行をモニタすることで，内部システムへの不審なアクセスを検知することができます．アカウントの不正利用によるシステム内部への侵入を防ぎます.	16 （検出）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります.	17 19 （反応）
					開発者により本番環境へのアクセスされるのを防ぎます．自社開発の成果物が本番環境からアクセスされるのを防ぎます.	18.9
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20 （復旧）
22	No.22	（-3）		システムを侵害し，重要データを改ざんすることで組織の信頼性を侵害	デバイスまたはソフトウェアのインベントリを適切に作成しておくことで，不正なデバイス及びソフトウェアを検出し，システムへの侵害を防止できる可能性があります.	1 2 （特定）
					ファイル完全性チェックツールを使用し重要システムファイルの変更の有無を確認することで機密文書への改ざんを検出できる可能性があります．ACLなどのセキュアな設定を施し，重要データへの不正アクセスを防ぎます.	5.1-5.2 5.4-5.5 （防御）
					システムの脆弱性が悪用され，システムが侵害される場合があります．脆弱性診断を継続実施することでリスクを低減することができます.	3 （防御）
					管理者権限の不正利用によるシステム侵害を防ぎます.	4
					SIEMツールまたはログ分析ツールを適用し，監視することで改ざんを検出できる可能性があります．このため，ログの適切な管理を実施することが望まれます.	6 （検出）
					メール及びWeb経由でシステムが侵害されることがあります．このため，電子メールとWebブラウザの保護によりシステムの侵害を防ぐことができます.	7 （防御）
					マルウェアを用いてシステムが侵害される場合があります．アンチウイルスソフトウェア等のマルウェア対策により侵害を防ぐことができます.	8 （防御）
					ポート，プロトコル，サービスの通信を悪用してシステムに侵害を受ける可能性があります．適切なサービス等の制限，コントロールが望まれます.	9 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします.	10 （復旧）
					ネットワークの通信設定をセキュアにすることで，不正アクセスによる侵入のリスクを低減します.	11.1-11.3
					信頼できない外部システム経由でシステムが侵害される場合があります．ネットワーク境界上にセキュリティ装置を配置し，システムを侵害する攻撃のリスクを低減することができます.	12.1-12.10 （防御）
					重要データを特定し，暗号化や完全性コントロールを実施することで，リスクを低減することができます.	**13(関連大)** （防御）
					情報を重要度に応じて，ネットワークを分割し，信頼度に基づいた適切な対応を実施することで，重要データが改ざんされるリスクを低減できます.	**14(関連大)** （防御）
					無線アクセス可能なデバイス経由でシステムに侵害されるのを防ぐため，認証や暗号化等の適切な無線アクセスコントロールにより，リスクを低減することができます.	15 （防御）
					アカウント管理の脆弱性を悪用し，システムを侵害される場合があります．適切なアカウントの監視，コントロールの実施が望まれます.	16 （防御）
					Webアプリケーション等の脆弱性が悪用され，システム侵害及びデータ改ざんが生起する場合があります．このため，適切なアプリケーションソフトウェアセキュリティの管理が望まれます.	18 （防御）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります.	17 19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20 （復旧）
23	No.23	（-3）		効果的対応能力を持たない組織内で検知されずに活動を継続	デバイスまたはソフトウェアのインベントリを適切に作成しておくことで，不正なデバイス及びソフトウェアを検出することができます.	1 2 （特定）
					管理者権限の不正利用を検知できます.	4.8-4.9
					SIEMツールまたはログ分析ツールを適用し，監視することで不正アクセスを検出できる可能性があります.	6.5-6.8 （検出）
					メール及びWeb経由で内部システムに侵入のためのマルウェアが送付される場合があります．不審メール，URLのフィルタリングを実施し，監視することでリスクを低減できます.	7.4-7.10 （検出）
					マルウェアを用いた内部システムへの侵入される場合があります．アンチウイルスソフトウェア等のマルウェア対策により検知できる可能性があります.	8.1-8.3 8.6 8.8 （防御）
					許可された通信以外をドロップする拒否ルールを持つホストベースファイアウォールなどをホストに適用し，監視することでリスクを低減することができます.	9.4 （防御）
					攻撃が成功した場合，システムが汚染されます．汚染されたシステムを完全に元の状態に修復することは非常に困難です．このため，定期的にデータをバックアップすることで汚染前の状態に復元できるようにします.	10 （復旧）
					信頼できない外部システム経由で内部システムに侵入される場合があります．ネットワーク境界上にセキュリティ装置を配置し，通信情報を収集・監視することでリスクを低減することができます.	12.1-12.8 12.12 （防御）
					監査ロギングを取得することで，非公開データへのアクセスを検知できる可能性があります.	14.5 14.9 （防御）
					不正に接続された無線アクセスポイントを検知できます.	15.1-15.3

					監査ログによって存在しないアカウントへのアクセスの試行をモニタすることで，内部システムへの不審なアクセスを検知することができます．	16.12 16.13 （検出）
					攻撃が成功した場合，迅速な対応が望まれます．インシデントレスポンスに係る事前の取り決めや訓練は被害の低減に繋がります．	17.1-17.3 17.9 **19(関連大)** （反応）
					WAFによりWebアプリケーションへの攻撃を検知できます．	18.10 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
			Type B		攻撃カードType Bはサイバーキルチェーン段階ごとの攻撃手法がまとめられています．このため，Type Aに比べて対応する防御カードは限定されます．	
		（-1）	初期偵察	（参考）	電子メール及びWebメールは攻撃の入口でよく悪用されます．また，攻撃者はシステムが利用しているサービスを掌握し，以降の攻撃に備えます．	**7 9** **（関連大）** （防御）
24	1.1	（-1）	初期偵察：発掘	システム情報の解明のため，対象から返答される未処理の例外やエラーメッセージを調査	事前に脆弱性スキャンを実施し，未処理の例外の有無を調査し，改善します．	3.1-3.2 3.6-3.7 （防御）
					不要なサービスへのアクセスを制御することで不必要な情報の開示を防止します．	9 11.1-11.3 （防御）
					WSDL（Web Services Description Language）ファイルを保護またはWSDLファイルへのアクセスを制限します．	14.6 （防御）
					Webアプリケーションのエラーメッセージの調査を目的と考える攻撃通信をWAFにより防御します．	18.10 （防御）
					エラー/レスポンス出力を機能的な使用または訂正に必要なものだけの最小限のものにする必要があります．また，アプリケーションの機能に必要でない機密情報を削除，エラーの「コード化」とコードとの紐付けが可能なコードブックによる識別は具体的な対策です．空白のindex.htmlを使用（空のindex.htmlを置くだけでディレクトリのリストがサイト訪問者に表示されない）することも有効です．	**18.6-18.8** **（関連大）** （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					堅牢な物理的セキュリティにより攻撃者がキーロガーをインストールする機会を低下させます．	その他
25	1.2	（-1）	初期偵察：傍受	システムにアクセス可能な媒体を介してデータを傍受	ネットワークに接続したスニファ（デバイス）を検出します．このため，デバイスの適正な資産管理を実施し，不正なデバイスを検出する必要があります．	**1** （特定）
					未許可の外部デバイス経由により，情報の収集を防ぎます．	**8.4-8.5**
					暗号化を利用してデータの送信を暗号化し，許可された者のみがアクセスできるようにします．ネットワーク構成管理用セグメントを業務システムと切り離すことで，データ傍受を防ぎます．	4.5 10.4 11.5 11.7 13.6-13.9 14.4 15.7 16.5 （防御）
					情報の重要度に応じてネットワークを分割しておくことで傍受可能となる情報を制限します．また，定期的にアクセスしないアーカイブデータ等への切り離すことで，リスクを低減できます．	14 15.10 （防御）
					不要な無線アクセス機能を無効化します．	15.4-15.6 15.9 （防御）
					認証機能により，無線ネットワークによる不正利用を防ぎます．	15.8 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
26	1.3	（-1）	初期偵察：フットプリンティング	システムまたはアプリケーションが送信する識別可能な情報を調査	ファイルとフォルダに対する適切なアクセス許可を設定します．標準的なセキュア設定を確立し，この設定を反映，維持する必要があります．場合によっては，識別可能情報を送信しないように設定します．	5.1-5.2 5.4-5.5 （防御）
					一般的なネットワーク脆弱性スキャンツールはシステム等から送信される識別情報とベースラインを比較し，既知の脆弱性を発見する場合があります．パッチを可能な限り毎週または毎日インストールして最新の状態に保ち，その後の攻撃段階への進行を防ぎます．	3 （防御）
					ネットワーク機器に強力なパスワードを選択してデフォルトのパスワードを変更することで，ネットワーク機器の識別可能情報とデフォルトパスワードの紐付けを阻止します．その後の攻撃段階への進行を防ぎます．	4.2 （防御）
					ネットワーク境界のログを定期的に調査することで，調査目的と思われる不審なアクセスを発見できる場合があります．	6.5-6.8
					ブラウザが送信するUser Agent等の情報により脆弱なブラウザが狙われる場合があります．最新のブラウザに保つことで，その後の攻撃段階への進行を防ぎます．	7.1
					不要なサービス/ポートを無効化し，識別可能な情報を制限します．不要なサービスの悪用のリスクを低減します．また，インターネットから接続できるサービスを制限します．	**9** （防御）
					ネットワーク機器の設定を確認し，不許可の設定追加により，悪用可能なアプリケーションの特定を防ぎます．	11.1-11.3

					効率的な識別可能情報の分析のために使用されるネットワーク脆弱性スキャナを使用する調査を識別・防御するために既知の悪意のあるIPを遮断します．また，IDS等で異常通信を識別します．	12.1-12.8
					一般的なネットワーク脆弱性スキャンツールはシステム等から送信される識別情報とベースラインを比較し，既知の脆弱性を発見する場合があります．WAFの使用やアプリケーションソフトウェアのセキュアなバージョンにより，その後の攻撃段階への進行を防ぎます．定期的なスキャンにより脆弱性を修正し，その後の攻撃段階への進行を防ぎます．	18.1 18.3 18.10 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1 20.3 20.5
					その他の具体的な対策としてWiFi MACアドレスの自動ランダム化，ハンドセットと再送信装置の頻繁な変更，ネットワーククローキング機能の無効化，頻繁にSSIDを新しい値と無関係な値に変更，携帯番号の頻繁な変更等が考えられます．	その他 （防御）
27	1.4	（-1）	初期偵察：プロトコル分析	システムが使用する通信プロトコルの情報を調査・解読	脆弱性診断により，脆弱なプロトコル（Telnetの非暗号通信等）の使用を発見し，使用を禁止または制限します．	3.1-3.2 3.6-3.7 （防御）
					不要なサービス/ポートを無効化し，脆弱なプロトコルの使用を制限します．脆弱なサービスの悪用のリスクを低減します．また，インターネットから接続できるサービスを制限します．	**9** （防御）
					ネットワーク機器の設定を確認し，不許可の設定追加により，脆弱なプロトコルの使用を防ぎます．	11.1-11.3
					脆弱なプロトコルの使用をIDS・IPSを使用して，発見できます．	12.6-12.7
					通信の暗号化により，通信プロトコルの解読を困難にします．	11.5 16.5 （防御）
					証明された暗号アルゴリズムを推奨キーサイズで使用する．不許可の無線機能を制限し，脆弱なプロトコルの使用のリスクを制限する．	15.6-15.9 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
28	1.5	（-1）	初期偵察：フィンガープリント	標的からの出力と既知のインジケータを比較し，標的を特定	OSやソフトウェアにパッチ適用します．悪意のある脆弱性スキャンと区別できるようにします．	3 （防御）
					Javascriptによりブラウザやバージョンを判定し，脆弱性を悪用する方法が用いられる場合があります．このため，ブラウザでJavascriptを無効化します．	7.1-7.3 （防御）
					不要なサービス/ポートを無効化し，識別可能な情報を制限します．不要なサービスの悪用のリスクを低減します．また，インターネットから接続できるサービスを制限します．例えば，ICMPによるOS推定を防ぐため，必要に応じてICMPを遮断します．	**9** （防御）
					ネットワーク機器の設定を確認し，不許可の設定追加による不要な通信の使用を防ぎます．	11.1-11.3
					脆弱性スキャナを使用する調査を識別・防御するために既知の悪意のあるIPを遮断します．また，IDS等で異常通信を識別します．IDSではnmap等のツールの使用を検知できます．	12.1-12.8
					一部の情報はプロトコルに基づいてシステムによって自動的に共有されていますが，可能な限りアプリケーションの機能には必要でない情報を削除します．すべてのコンテンツの入力及び出力検証します．HTTP応答のサーバーフィールドを難読化，HTTP応答ヘッダーの内部順序を非表示，404または500などのHTTPエラーコードのカスタマイズ，URLファイルの拡張子を非表示，HTTP応答ヘッダーソフトウェア情報を非表示，Cookieのソフトウェア情報の隠蔽，データベースAPIのエラーメッセージのデータベースタイプを難読化が具体的な対策です．	18.1-18.4 18.6 18.8 18.10 18.11 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
29	1.6	（-1）	初期偵察：情報抽出	ソーシャルエンジニアリリングにより，標的組織及び個人に関する重要な情報を取得	ネットワーク境界のログを定期的に調査することで，不審なサイトへのアクセス，不審メールを発見できる場合があります．	6.5-6.8
					URLフィルタリングにより，業務と無関係なサイトへのアクセスを禁止します．スクリプトを無効化し，ポップアップの表示等による人間の心理的な脆弱性を突く攻撃のリスクを低減します．URLのリクエストログを取得し，不審なサイトへのアクセスの有無を確認します．SPFの使用により，なりすますメールを検出します．	**7 関連大** （防御）
					従業員に定期的に堅牢なサイバーセキュリティトレーニングを提供します．機密情報の提供を求める電子メールへの返信等を防ぐことができます．	**17** （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
		（-1）	ツール開発/取得	（参考）	攻撃者は効果的に攻撃を実施するため，攻撃ツールを使用しマルウェアの作成する場合があります．この場合，既存の脆弱性が未対応のシステムを攻撃する場合が一般的です．このため，診断により，事前に脆弱性を修正しておく必要があります．	4 （特定）
					ツールは専用のデバイスまたはソフトウェアにより実行させる可能性があります．このため，デバイス及びソフトウェアの適正な資産管理を実施し，不正なデバイス，ソフトウェアを検出する必要があります．	1 2 （特定）
					ツールにより悪用される可能性があるセキュリティ設定の脆弱性のリスクを低減します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性スキャンにより，悪用可能な脆弱性を事前に特定，修復する必要があります．	**3 関連大** （特定）
					ツールを使用すると本来で生成されない異常なログが記録される場合があります．収集されたログを分析することで不審な挙動を検出できます．	6 （検出）
					電子メールやWebブラウザからツールにより作成された悪意のあるコードを実行してしまう場合があります．このため，電子メール及びWebブラウザの不要な機能を制限することが望まれます．	7.1-7.3 7.9-7.10 （防御）

30	2.1	(-1)	ツール開発/取得	攻撃の効率化を図るため，ツールを開発または取得し，使用	ツールを使用し，作成したマルウェアやExploitはアンチウィルスソフトで対応済みの場合があります．また，外部デバイス経由でのツールの実行を防止します．	8 （検出）
					不要なサービス/ポートを無効化し，ツールにより収集される情報を制限します．ツールによる不要なサービスの悪用されるリスクを低減します．	9
					ネットワーク機器のセキュアな設定により，ネットワーク経由でのツール悪用のリスクを低減します．	11.1-11.3
					ツールは特徴的な通信を含む場合があるため，IDS，IPSにより不審通信の検知・防御が可能です．	12.1-12.8 （防御）
					無線通信の脆弱性を突くツールによる攻撃のリスクを低減します．	15
					ツールを用いた認証情報の取得する攻撃へのリスクを低減します．	16.4-16.6 16.8-16.10 16.12 16.13
					ツールは特徴的な通信を含む場合があるためWAFにより不審通信の検知・防御が可能です．ツールによって悪用される恐れがある脆弱性を発見・修正することで，リスクを低減します．	18.1-18.8 18.10 18.11 （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．既存のツールを用いることで，ツールによる攻撃成功の可能性を確認できます．	20.1-20.3 20.5-20.7
		(-1)	配送	（参考）	電子メール及びWebは攻撃の入口でよく悪用されます．攻撃者は悪意のあるコードを電子メール及びWeb経由により標的に配送しますが，セキュリティ機能により防御できる可能性があります．	7 （防御）
					攻撃者は巧みに悪意のあるコードを標的に実行させようとします．セキュリティのトレーニングにより，攻撃者の罠を見破ることができる可能性があります．	17 （検出）
31	3.1	(-1)	配送：コンテンツスプーフィング	フィッシングサイト等の偽装コンテンツを表示	ネットワーク境界のログを定期的に調査することで，不審なサイトへのアクセスを発見できる場合があります．	6.5-6.8
					不要なスクリプトの起動を防止するためにフィッシングサイトのコンテンツ内の悪意のあるスクリプトの実行を防ぐことができます．URLリクエストログを取得し，フィッシングサイトへのアクセスの有無を確認します．URLフィルタリングにより，不審なサイトへのアクセスを防止します．	**7** **関連大** （防御）
					ウイルス定義ファイルの更新を確認します．必要に応じ，マルウェアのカスタムシグネチャの作成，ヒューリスティックベースのマルウェア検出技術を用います．偽装コンテンツからダウンロードする可能性がある悪意のあるコードを検出できる場合があります．	8.1-8.2 （防御）
					既知の悪意のあるURLへの接続を防止します．偽装コンテンツからダウンロードする可能性がある悪意のあるコードをIDS・IPSで検出できる場合があります．プロキシ経由のアクセスにすることでアクセスログを集約し，ログ解析を容易にします．	12.1 12.6-12.7 12.9-12.10 （防御）
					フィッシングサイト等の特徴を従業員に教育し，把握させることが重要です．従業員にUDDI，ebXMLまたは信用できる当事者によって検証可能な形で署名された同様のメッセージのみを信頼するように教育することも重要です．	**17** **関連大** （防御）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．レッドチームは標的型メール攻撃等を実施し，受信者の反応を確認します．	20.1-20.3 20.5-20.7
32	3.2	(-1)	配送：アイデンティティスプーフィング	窃取またはなりすました認証情報を使用し，メッセージや署名付きファイルを送付	最新のパッチの適用を適用することで，危殆化したハッシュアルゴリズムに警告を表示する等により，信頼性のないサイト等を識別できる可能性があります．	3.4-3.5 （防御）
					ネットワーク境界のログを定期的に調査することで，不審なサイトへのアクセスを発見できる場合があります．	6.5-6.8
					S/MIME対応の最新メーラの使用することで，リスクを低減します．Sender Policy Framework（SPF）の実装によりリスクを低減します．	**7.1 7.8** **関連大** （防御）
					すべてのリモートメソッドの保護を確認することで認証情報を保護します．	11.5 12.11 15.8 （防御）
					信頼できるサイトのみにアクセスを制限し，脆弱な証明書を偽装するサイトへアクセスするリスクを低減します．プロキシ経由のアクセスにすることでアクセスログを集約し，ログ解析を容易にします．	7.4-7.5 12.1 12.3 12.9
					非監視アカウントからの秘密鍵へのアクセスを制限します．	14.6
					全パスワードを暗号化することで，認証情報への不正アクセスのリスクを低減します．使い回しの認証情報を悪用し，フリーメールサービスによるなりすましメールの送信を防ぎます．	16.4
					社内でポリシーに反する要求には対応しないように教育をすることが重要です．例えば，機密情報の提供を求める電子メールには絶対に返信しないこと等があげられます．	**17** **関連大** （検出）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					DNSへの依存を避け，ホストファイル/ IPアドレスを含める，DNSSECの利用，SHA-256やSHA-512などのより強力なハッシュ関数を使用し，署名しようとしている証明書をハッシュする，よく知られている認証局から発行された有効な証明書との安全な接続を介し，信頼できるWebサイトにのみ機密情報を提供する等がその他の具体的な対策です．	その他 （防御）
					ネットワーク境界のログを定期的に調査することで，不審なサイトへのアクセスを発見できる場合があります．	6.5-6.8
					対策が取られた最新のブラウザを使用します．悪意のあるサイトはURLフィルタリングやスクリプトの制限により防御できる場合があります．例えば，Javascriptでリンクのアドレスバーの偽装が可能です．不要なスクリプトを無効化することが重要です．なりすましメールを介して悪用されること場合が多いことから，SPFも有効です．	**7** **関連大** （防御）

33	3.3	(-1)	配送:リソースロケーションスプーフィング	ブラウザに偽のアドレスを表示する等により利用者が意図しない場所からリソースを取得	信頼できるサイトのみにアクセスを制限し，脆弱な証明書を偽装するサイトへアクセスするリスクを低減します．プロキシ経由のアクセスにすることでアクセスログを集約し，ログ解析を容易にします．	7.4-7.5 12.1 12.3 12.9 (防御)
					例えば，EV SSLサーバー証明書を使用したサイトはブラウザのアドレスバーが緑色の表示になる場合があります．教育により，アドレスバーから信頼できるサイトか判断することができます．なりすましメールを介して悪用されること場合が多いことから，不審メール訓練も有効です．	**17** **関連大** (検出)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					その他の対策として，DNSホスト名を使用する場合，すべてのサーバーを認証し，冗長チェックを実行することが考えられます．	その他
34	3.4	(-1)	配送:アクションスプーフィング	目に見えないインターフェースを利用して意図しない動作を実行	ネットワーク境界のログを定期的に調査することで，不審なサイトへのアクセスを発見できる場合があります．	6.5-6.8
					対策が取られた最新のブラウザを使用します．悪意のあるサイトはURLフィルタリングやスクリプトの制限により防御できる場合があります．なりすましメールを介して悪用されること場合が多いことから，SPFも有効です．Webページに難読化したiFrameを埋め込み，不審なサイトへ転送する方法がよく用いられます．このため，iFrameを難読化するスクリプトの無効化が有効です．また，必要に応じ，iFrameタグの無効化します．例えば，Firefoxブラウザを使用している場合，iFrameを禁止するためのNoScriptプラグインを使用します．また，不審なURLをブロックすることが重要です．	**7** **関連大** (防御)
					信頼できるサイトのみにアクセスを制限し，脆弱な証明書を偽装するサイトへアクセスするリスクを低減します．プロキシ経由のアクセスにすることでアクセスログを集約し，ログ解析を容易にします．	7.4-7.5 12.1 12.3 12.9 (防御)
					従業員に定期的で堅牢なトレーニングを提供します．疑わしいサイトとのやりとりや疑わしいリンクのクリックは避けることができるようになります．	**17** **関連大** (防御)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
35	3.5	(-1)	配送:人間の行動を操作	人間の心理につけこみ，標的から情報を収集または標的を操作して利益を獲得	許可されていない重要ファイルの変更，設定変更を検知します．	5.5
					管理アカウントインベントリから管理権限ユーザの上級管理者による承認を確認することで管理者アクセスの悪用を防止できる可能性があります．不正な管理者アカウントの追加を防ぎます．	4.8-4.9 (防御)
					装置のログを定期的に調査することで，不審なサイトへのアクセスを発見できる場合があります．	6.5-6.8
					URLフィルタリングにより，業務と無関係なサイトへのアクセスを禁止します．スクリプトを無効化し，ポップアップの表示等による人間の心理的な脆弱性を突く攻撃のリスクを低減します．URLのリクエストログを取得し，不審なサイトへのアクセスの有無を確認しま	**7.2-7.10** **関連大**
					信頼できるサイトのみのアクセスを許可し，人間の心理につけこむ不審なサイトへのアクセスを制限します．プロキシ経由のアクセスにすることでアクセスログを集約し，ログ解析を容易にします．	12.3 12.9
					従業員に定期的で堅牢なトレーニングを提供します．不要な情報の共有を避けることができます．	**17.1-17.4** **17.7-17.9** **関連大**
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
		(-2)	初期侵害	(参考)	初期侵害は攻撃者が用意したデバイスまたはソフトウェアの実行される場合があります．このため，デバイス及びソフトウェアのインベントリ情報を適切に管理し，不正なデバイス，ソフトウェアを検出する必要があります．	1 2 (特定)
					攻撃者は設定の不備，メール，Web，サービス，マルウェア，アプリケーションといった様々な経路を使ってシステムの侵害を試みます．これらの設定やセキュリティ装置を組み合わせることで効果的に防御が実現可能です．	3 7 8 11 15 18 (防御)
					攻撃経路の脆弱性は継続的な診断によって検出可能です．また，装置のログを収集・監視・分析することで，サイバー攻撃を検出できます．エンドポイントにはマルウェア対策が効果的です．	4 6 8 (検出)
					システムに脆弱性が発見された場合はシステムへの影響を考慮し，迅速に対応を決定する必要があります．	4 (反応)
36	4.1	(-2)	初期侵害:防御回避	シグネチャベースによる検出回避のため，バイナリパディングによりファイルハッシュを変更	悪意のあるソフトウェアを特定し，AppLockerまたはソフトウェア制限ポリシーなどのホワイトリストツールを使用して監査またはブロックします．各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります．	**2** **関連大** (特定)
					OSで収集された監査ログの分析により，不審なファイルの実行を検出できる可能性があります．	**6** **関連大** (検出)
					悪意のある難読化JavaScriptの生成過程で無意味な情報を追加することにより，シグネチャ検知を回避する．JavaScript等のスクリプトを無効化することでリスクを低減できる．	**7.1-7.5** **関連大**
					レピュテーション機能やEMETを活用することもできます．ファイルをパッドするために使用される方法に応じて，スキャンまたはオンアクセスベースのツールを使用してパディングを検出できる場合があります．	**8.1-8.3** **関連大** (防御)
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 (復旧)
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 (反応)

					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
37	4.2	(-2)	初期侵害: 防御回避	形跡を消すため, レジストリ・コマンド ヒストリ・イベント ファイル・マルウェア自身等を削除	悪意のあるソフトウェアを特定し, AppLockerまたはソフトウェア制限ポリシーなどのホワイトリストツールを使用して監査またはブロックします. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります.	**2** **関連大** (防御)
					ユーザーが特定のファイルを削除または書き込みできないようにすることで悪意のある変更することを防ぐことが可能です. このため, ファイル等へのアクセス制限を適切に実施するため, ソフトウェアにセキュアな設定を施す必要があります.	**5.1-5.2** **5.4-5.5** **関連大** (防御)
					設定の不備(アクセス制御設定の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	**3.1-3.2** **3.6 -3.7** (検出)
					レジストリ等の変更が実施可能な管理権限による作業を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また, 管理者権限アカウント使用者が判別できるようにする必要があります.	4 (防御)
					OSで収集された監査ログの分析により, 不審なファイルの実行を検出できる可能性があります. HISTFILEおよびHISTFILESIZE環境変数の変更, ～/.bash_historyファイルの削除/クリアは疑わしい活動の指標となります.	**6** **関連大** (検出)
					悪意のあるマルウェアはマルウェア対策で検出・防御できる可能性があります.	**8.1-8.3 8.6** **関連大** (防御)
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 (復旧)
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
38	4.3	(-2)	初期侵害: 防御回避	OSやアプリケーションの機能を利用し, セキュリティツールによる悪意のある動作の検出を防止	AppLockerまたはソフトウェア制限ポリシーなどのホワイトリストツールを使用して, DLLインジェクション機能を含む可能性のある悪質なソフトウェアを特定またはブロックします. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります.	**2** **関連大** (防御)
					OSやアプリケーションの機能の制限するための設定を施し, リスクを低減できます.	**5.1-5.2** **5.4-5.5** **関連大**
					設定の不備(OS等有効機能の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	**3.1-3.2** **3.6 -3.7** **関連大** (検出)
					OSで収集された監査ログの分析により, 不審なファイルの実行を検出できる可能性があります. 様々なタイプのコードインジェクションを示すAPI呼び出しを呼び出すとかなりの量のデータが生成される可能性があり, 通常のAPI関数と異なるため, 悪意のある行為と区別可能な場合があります.	**6** **関連大** (検出)
					電子メール及びブラウザの機能を悪用する場合があります. 不要なアドオン, スクリプトを無効化することが有効です.	**7.1-7.3** **関連大** (防御)
					悪意のあるファイルを利用している場合, マルウェア対策が有効です.	**8.1-8.3 8.6** **関連大** (防御)
					クライアントまたはサーバの機能で起動可能な不必要なサービスが悪用される場合があります. 定期的に堅牢な状態が維持されていることを確認します.	9.1-9.4
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 (復旧)
					ネットワーク機器のセキュアな設定により, OSの機能で起動可能な不必要なネットワークサービスの悪用のリスクを低減します.	**11.1-11.3** **関連大**
					境界ネットワーク上のセキュリティ装置へのカスタムシグネチャの適用やアノマリ検知の閾値調整なので, 通常では検知できない悪意のある動作を検出できる場合があります. 未許可のネットワークサービスの利用を検知できます.	12.6-12.8
					無線クライアントの機能を制限することで, 未許可の機能を悪用されるリスクを低減します.	**15.6 15.9** **関連大**
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
39	4.4	(-2)	初期侵害: 防御回避	悪意のあるコードを難読化・暗号化し, コードの分析から回避	ホワイトリストツールを使用して、パックされている可能性のある悪質なソフトウェアの特定と防止します. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります.	**2** **関連大** (防御)
					OSで収集された監査ログの分析により, 不審なファイルの実行を検出できる可能性があります. 難読化自体の検出が不可能な場合, 難読化されたファイル実行時の悪意のある行為(例えば, ファイルシステム上のファイルの書き込み, 読み取り, または変更に使用された方法)を検出することが可能です.	**6** **関連大** (検出)
					特にブラウザ上で実行される悪意あるコードが難読化されている場合があります. スクリプトの実行を防止することで, 難読化された悪意のあるコードが実行される可能性を低減できます.	**7.1-7.3** **7.9 7.10** **関連大** (防御)
					最新のウイルス定義を使用することが基本です. ファイルスキャンを使用して, 既知のソフトウェアパッカーやパッキング手法の成果物を探索します.	**8.1-8.3 8.6** (防御)

					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					IDSまたはIPSにより難読化スクリプトの使用を検知できます.	12.6-12.7
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
40	4.5	（-2）	初期侵害：防御回避	悪意のあるプログラムのタイムスタンプを改ざんし，分析から回避	AppLockerやソフトウェア制限ポリシーなどのホワイトリストツールを使用して，タイムスタンプを実行する機能を含む可能性のある悪質なソフトウェアを特定し，ブロックします. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります.	**2** **関連大** （防御）
					ユーザーが特定のログファイルを削除または書き込みできないようにすることで悪意のある変更することを防ぐことが可能です. このため，ファイル等へのアクセス制限を適切に実施するため，ソフトウェアにセキュアな設定を施す必要があります.	**5.1-5.2** **5.4-5.5** **関連大** （防御）
					設定の不備(アクセス制御設定の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	**3.1-3.2** **3.6-3.7** **関連大** （検出）
					ログファイル等の変更が実施可能な管理権限による作業を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また，管理者権限アカウント使用者が判別できるようにする必要があります.	4 （防御）
					ログの分析によりタイムスタンプの改ざんを検出できる場合があります. タイムスタンプが変更されたファイルの側面を検出するためのフォレンジック手法が存在します. また，ファイルハンドルのオープンに関する情報を収集し，タイムスタンプの値を比較可能なファイル変更監視を使用します.	**6** **関連大** （検出）
					悪意のあるプログラムを利用している場合，マルウェア対策が有効です.	**8.1-8.3 8.6** **関連大** （検出）
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
41	4.6	（-2）	初期侵害：防御回避	セキュリティツールを無効化し，悪意のあるアクティビティの検出を回避	AppLockerやソフトウェア制限ポリシーなどのホワイトリストツールを使用して，セキュリティツールを無効化する機能を含む可能性のある悪質なソフトウェアを特定し，ブロックします. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審なソフトウェアの実行を検出できる可能性があります.	**2** **関連大** （防御）
					セキュリティサービスを無効化されないように，適切なプロセス，レジストリおよびファイルのアクセス許可が設定されていることを確認します. ソフトウェアへのセキュアな設定が有効です. 内部犯によるセキュリティ装置上の重要システムファイルの変更有無を監視します.	**5.1-5.2** **5.4-5.5** **関連大** （防御）
					設定の不備(アクセス制御設定の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	**3.1-3.2** **3.6-3.7** **関連大** （検出）
					レジストリ等の変更が実施可能な管理権限による作業を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また，管理者権限アカウント使用者が判別できるようにする必要があります.	4 （防御）
					ログの分析によりセキュリティツールの無効化を検出できる場合があります. プロセスとコマンドライン引数を監視してセキュリティツールが強制終了または停止されていないか確認します.	**6** **関連大** （検出）
					悪意のあるアクティビティがマルウェアを使用している場合，マルウェア対策が有効です. 継続的にセキュリティツールの稼働状況をモニタします.	**8.1-8.3 8.6** **関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					内部犯により，ネットワークセキュリティ機器を無効化される場合があります. この場合，設定の変更を検知することで，不正を識別できます.	11.3
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
					ソフトウェアの棚卸しを適切に実施し，無許可のソフトウェアの使用を防止します. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審な操作を検出できる可能性があります.	**2** **関連大** （防御）
					ネットワーク管理目的で使用するソフトウェアのセキュアな設定を施し，悪用を防止します. 許可された管理者だけにアプリケーション導入システムへのアクセスを許可します.	**5.1-5.2** **5.4-5.5** **関連大** （防御）
					設定の不備よるソフトウェアの脆弱性は継続的な脆弱性診断によって検出可能です. 定期的にアプリケーションへのパッチを適用することも重要です.	**3.1-3.2** **3.4-3.7** **関連大** （検出）
					管理権限を使用したソフトウェアによる実行可能な処理を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また，管理者権限アカウント使用者が判別できるようにする必要があります.	4 （防御）

42	4.7	(−2)	初期侵害：実行	ネットワーク管理目的で使用するサードパーティアプリケーションやソフトウェア開発システムを悪用し，制御コードを実行	ログの収集分析により，悪用を検出ができる可能性があります．ログを収集して環境の他のデータと関連付けを実施します．既知の良性ソフトウェアと相関のないプロセス活動を監視します．展開システムのアカウントログインアクティビティを監視します．	**6** **関連大** （検出）
					悪意のあるアクティビティがマルウェアを使用している場合，マルウェア対策が有効です．継続的にセキュリティツールの稼働状況をモニタします．	**8.1−8.3 8.6** **関連大** （防御）
					ネットワーク経由による悪用を防止するため，ファイアウォールの使用や検証されたサービス等のみが稼働していることを確認します．	9 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					ネットワーク機器のセキュアな設定を施します．多要素認証や強固なパスワードの使用により悪用のリスクを低減します．管理用セグメントのみのアクセスを許可し，悪用のリスクを低減します．	**11** **関連大** （防御）
					ファイアウォール等のネットワーク境界のセキュリティ装置を使用し，不審な通信を検知・防御します．リモートログインには多要素認証を用います．	12.1−12.8 12.11 12.12 （防御）
					重要なネットワークシステムへのアクセスを分離し，悪用による被害を最小限に留めます．ファイルシステムへのアクセス制御により，リスクを低減します．	14.1−14.3 （防御）
					開発システムにアクセスするために使用されるアカウントの資格情報が一意であり，企業ネットワーク全体で使用されていないことを確認します．また，開発システムの悪用を防止するため，セキュアなコードを書けるように訓練します．	**18.6 18.9** **関連大** （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					サードパーティ製ソフトウェアのセキュリティを評価を含むペネトレーションテストが有効です．	20.1−20.3 20.5−20.7
43	4.8	(−2)	初期侵害：実行	開発，デバッグ，リバースエンジニアリングを支援するソフトウェア関連ユーティリティを悪用し，悪意のあるコードを実行	ソフトウェアの棚卸しにより，不要なソフトウェアを削除します．アプリケーションホワイトリストを使用します．無許可のソフトウェアの使用を防止します．また，許可されたソフトウェアの使用はログにより，監視します．	**2** **関連大** （防御）
					特定のファイルへのアクセスを監視することで，不審な挙動を検出できる可能性があります．例えば，MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe，cdb.exeおよびtracker.exeの実行と引数を監視します．	**6** **関連大** （検出）
					悪意のあるアクティビティがマルウェアを使用している場合，マルウェア対策が有効です．継続的にセキュリティツールの稼働状況をモニタします．	**8.1−8.3 8.6** **関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					重要なネットワークシステムへのアクセスを分離し，悪用による被害を最小限に留めます．開発等のユーティリティを含むネットワークを分離します．ファイルシステムへのアクセス制御により，リスクを低減します．	14.1−14.3 14.6 （防御）
					開発システムにアクセスするために使用されるアカウントの資格情報が一意であり，企業ネットワーク全体で使用されていないことを確認します．また，開発システムの悪用を防止するため，セキュアなコードを書けるように訓練します．	**18.6 18.9** **関連大** （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1−20.3 20.5−20.7
44	4.9	(−2)	初期侵害：実行	標的が使用するOSやアプリケーションの機能・仕組みを悪用し，標的を制御するコードを実行	ホワイトリスト作成ツールを使用し，コマンドラインインタプリタや潜在的に悪質なソフトウェアを監査またはブロックします．また，使用が許可されたソフトウェアはログを収集します．	**2.7−2.9** **関連大** （防御）
					セキュアな設定（アクセス制限等）を施し，ユーザ権限で実行可能な機能を制限することで悪用のリスクを制限します．リモート管理の機能の悪用を防止します．重要ファイルの改ざんに気がつけるように完全性チェックツールを使用します．	**5.1−5.2** **5.4−5.5** **関連大** （防御）
					継続的な脆弱性診断により，適切な設定（アクセス制限等）を確認・修正し，悪用を制限します．	**3.1−3.2** **3.4−3.7** **関連大** （検出）
					PowerShell実行ポリシーを管理者に制限し，署名付きスクリプトのみの実行を許可します．このため，管理者権限の悪用を防止する必要があります．	4 （防御）
					監査ログの収集・監視により検出できる可能性があります．CUIのアクティビティはコマンドライン引数を使用したプロセス実行の適切なロギングが必要です．また，API監視によるAPI関数呼び出しのための動作と他のイベントとの相関します．PowerShellのログ機能を有効にし，監査します．	**6** **関連大** （検出）
					ブラウザ・メーラーで実行される悪意あるスクリプトの実行を防止します．難読化された悪意のあるコードが実行される可能性を低減できます．	**7.1−7.3** **7.9−7.10** **関連大** （防御）
					マイクロソフトの強化された緩和エクスペリエンスツールキット（EMET）やアタックサーフェスリダクション（ASR）機能といったマルウェア対策を施します．ホストの制御を企図するC2サーバへのアクセスを検知します．	**8.1−8.3** **8.6−8.7** **関連大** （防御）
					ポート，プロトコル，サービスを検証し，不要なサービス等はブロックします．定期的な確認を実施し，不要な機能の悪用によるリスクを低減できます．	9.1−9.4
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					ネットワーク機器のセキュアな設定により，OSの機能で起動可能な不必要なネットワークサービスの悪用のリスクを低減します．	**11.1−11.3** **関連大**

					境界ネットワークに配置したセキュリティ機器により，OSやアプリケーションの機能・仕組みを悪用を企図する不審な通信を検知・防御します．	12 （防御）
					不要な無線アクセス機能を無効化し，悪用を防ぎます．無線デバイスの不適切な設定を悪用されるのを防ぎます．	**15.4-15.6 15.9 関連大** （防御）
					PowerShell実行ポリシーを管理者に制限し，署名付きスクリプトのみの実行を許可します．アカウントの監視により，不正なアカウント利用を防ぎます．	16.1-16.3 16.6-16.10 16.12 16.13 （防御）
					外部に公開しているアプリケーションの適切な管理が望まれます．悪意のあるコードが実行されないようにWAFやセキュリティ設定により防御します．	**18.1-18.8 18.10 18.11 関連大** （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
		(-2)	誤用/特権昇格	（参考）	管理者権限のアクセス権を持っている人や作業について特定しておくことが重要です．	5 （特定）
					管理者権限を含むアカウントの不正使用を適切な管理により防御できます．また，取り扱う情報に応じてネットワークを分割しておくことで，攻撃を防御できます．	5 14 16 （防御）
					継続的な脆弱性診断により，システムの脆弱性を検出できます．また，監査ログやアンチウイルスソフトの検出機能を利用することで特権昇格攻撃を検知できます．	4 6 8 （検出）
					システムに脆弱性が発見された場合はシステムへの影響を考慮し，迅速に対応を決定する必要があります．	4 （反応）
45	5.1	(-3)	誤用/特権昇格	動的ライブラリの仕組みを利用し，他のプロセスに悪意のあるコードをロードさせ，実行	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，AppCert，DLLを通じて実行される潜在的な悪意のあるソフトウェアを特定し，ブロックします．また，許可されたソフトウェアはログで収集します．	2 （防御）
					ログを分析することで攻撃を検出できる可能性があります．AppCert，DLLsレジストリ値を監視し，既知のソフトウェア，パッチサイクルなどと相関のない変更を検出します．C2，収集，侵入拡大など，他のアクティビティにつながる一連の動作の一部として収集します．不明または異常なプロセスの起動を検出します．不明または異常なプロセスの起動を検出します．	**6 関連大** （検出）
					マイクロソフトの強化された緩和エクスペリエンスツールキット（EMET）やアタックサーフェスリダクション（ASR）機能といったマルウェア対策を施します．	**8.1-8.3 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
46	5.2	(-3)	誤用/特権昇格	不適切なファイルシステムのパーミッションを利用し，管理者権限で起動するプロセスをユーザ権限で改ざん	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，ファイル，ディレクトリおよびサービスのアクセス許可を悪用して実行される可能性のある悪意のあるソフトウェアを特定し，ブロックします．また，許可されたソフトウェアはログを取得します．ファイルダウンロードディレクトリやtempディレクトリなどのユーザディレクトリからの実行を拒否します．	2 （防御）
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．ファイルシステムのパーミッションに適切なアクセス許可が設定されていることを確認します．ユーザーアカウントとグループの権限を制限します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．不適切なファイルシステムのパーミッションによるアクセス許可をを検出できる監査ツールを使用します．	3.1-3.2 3.4-3.7 （検出）
					監査ログの分析により不審な挙動を検出できます．実行可能ファイルの書き込み，名前の変更，既存のサービス実行ファイルと一致するような移動を検出し，他の疑わしい動作と関連づけして検出します．	**6 関連大** （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.3 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					アカウントの不正利用を防止するため，アカウントの監視，管理を適切に実施します．	**16.1-16.3 16.6-16.10 16.12 16.13 関連大**
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，サービス濫用によって実行される潜在的な悪質なソフトウェアを特定し，ブロックします．また，許可されたソフトウェアはログを取得します．	2 （防御）

47	5.3	(-3)	誤用/特権昇格	不適切なレジストリのパーミッションを利用し，管理者権限で起動するプロセスを登録	セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．レジストリハイブに適切なアクセス許可が設定されていることを確認します．ユーザーアカウントとグループの権限を制限します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．不適切なレジストリハイブのアクセス許可を検出できる監査ツールを使用します．	3.1-3.2 3.4-3.7 （検出）
					管理者権限アカウントの不正利用を防ぎます．不正な操作を発見できるようにします．	**4** **関連大**
					監査ログの分析により不審な挙動を検出できます．C2，収集，侵入拡大など，他のアクティビティにつながる一連の動作の一部として検出します．	**6** **関連大** （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.3 8.6** **関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					管理者権限アカウントの不正利用を防止するため，アカウントの監視，管理を適切に実施します．	**16.1-16.3** **16.6-16.10** **16.12** **16.13** **関連大**
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
48	5.4	(-3)	誤用/特権昇格	資格情報アクセス技術を使用して，特定アカウントの資格情報を窃取	セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．ファイルシステムのパーミッションに適切なアクセス許可が設定されていることを確認します．ユーザーアカウントとグループの権限を制限します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．不適切なファイルシステムのパーミッションによるアクセス許可ををを検出できる監査ツールを使用します．	3.1-3.2 3.4-3.7 （検出）
					管理者権限の適切に管理します．特権エスカレーションの機会を制限します．不正な操作を発見できるようにします．	**4** **関連大** （防御）
					監査ログの解析により攻撃を検出できる可能性があります．コマンドラインの活動を監査することによってトークンの操作を検出します．他のエンドポイントとネットワークの動作との相関によってトークンの操作を検出します．	**6** **関連大** （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.3 8.6** **関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					資格情報にACLを設定し，アクセス時にログを取得することで，不審な操作に気づきます．	**14.6 14.9** **関連大**
					アカウントの管理を適切に実施します．攻撃者による認証情報の摂取を防ぎます．ユーザー，アカウントを業務に必要な最低限の権限に制限します．	**16** **関連大** （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
49	5.5	(-3)	誤用/特権昇格	OSやアプリケーションの機能または脆弱性を悪用し，アカウントの権限を昇格	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．レジストリハイブに適切なアクセス許可が設定されていることを確認します．ユーザーアカウントとグループの権限を制限します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．不適切なファイルシステムのパーミッションによるアクセス許可ををを検出できる監査ツールを使用します．	3.1-3.2 3.4-3.7 （検出）
					PowerShell実行ポリシーを管理者に制限し，署名付きスクリプトのみの実行を許可します．このため，管理者権限の悪用を防止する必要があります．アカウントの監視により，不正なアカウント利用を防ぎます．許可された管理者だけにアプリケーション導入システムへのアクセスを許可します．開発システムにアクセスするために使用されるアカウントの資格情報が一意であり，企業ネットワーク全体で使用されていないことを確認します．グループポリシーおよびマルチファクタ認証を使用します．アカウント特権を分離します．	**4** **16** **関連大** （防御）
					ログを分析することで攻撃を検出できる可能性があります．ソフトウェアの悪用により生成されたクラッシュした場合，ソフトウェアおよびOSのクラッシュレポートを参照します．追加のプロセスの起動やファイルへの読み書きなど，特定のプロセスには珍しい動作を検知します．	**6** **関連大** （検出）
					古いブラウザ等には特権昇格の脆弱性があります．サポートされたブラウザによりパッチの適用によりリスクを低減します．	7.1
					Microsoft Enhanced Mitigation Experience Toolkitなどの悪用防止ツールを使用し，発見されていない脆弱性またはパッチが適用されていない脆弱性を悪用して運用を進めるのを困難にします．マイクロソフトの強化されたアタックサーフェスリダクション（ASR）機能といったマルウェア対策を施します．	**8.1-8.3 8.6** **関連大** （防御）

					ポート，プロトコル，サービスを検証，不要なサービス等はブロックします．定期的な確認を実施し，リスクを低減できます．ファイアウォールの使用します．グループポリシーおよびマルチファクタ認証を使用します．	9.1-9.4 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					ポート，プロトコル，サービスを検証，不要なサービス等はブロック，定期的な確認を実施し，リスクを低減できます．ファイアウォールの使用します．グループポリシーおよびマルチファクタ認証を使用します．	11.1-11.3 （防御）
					プロキシを強制し，DNSなどのサービスに専用のプロキシを使用し，それぞれのポート/プロトコルを介して通信します．シグネチャを使用するネットワーク侵入検知および防止システムを使用して，ネットワークレベルでの不審なアクティビティのリスクを低減します．	12.1-12.10 （検出）
					SQLインジェクションによるWebアプリケーションの脆弱性の悪用等で任意のコマンドが実行される可能性があります．WAFや脆弱性診断による脆弱性修正により攻撃を防ぎます．	18.1-18.8 18.10 18.11 （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
		（-3）	内部偵察	（参考）	管理者権限を使用することで，より詳細なシステム情報を取得可能です．管理者権限のコントロールを適切に実施することで防御することができます．	5 （防御）
					内部偵察活動により，エンドポイントやネットワーク機器に様々なログ情報が生起します．これらのログを利用することで，内部偵察活動を検出できます．	6 （検出）
50	6.1	（-3）	内部偵察：資格情報アクセス	アカウント情報が保存されているファイルや履歴を調査	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用して監査またはブロックします．また，許可されたソフトウェアはログを取得します．	2 （防御）
					セキュアな設定（アクセス制限）により，防御できる場合があります．リモートユーザーのアクセス許可を制限します．アプリケーションがUACを介して昇格しているときに管理者アカウントが列挙しないようにします．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．不適切なファイルシステムのパーミッションによるアクセス許可をを検出できる監査ツールを使用します．	3.1-3.2 3.4-3.7 （検出）
					アカウント情報へのアクセスのため，管理者権限を使用する可能性があります．管理権限を最小限に抑え，必要な場合にのみ管理アカウントを使用します．また，管理者権限アクセスを監視します．	**4** **関連大** （防御）
					ログ分析により不審な挙動を検出できる可能性があります．取得した情報に基づいて，侵入拡大などの他のアクティビティにつながる一連の動作の一部として表示・分析します．実行中のプロセスのコマンドライン引数を監視して，疑わしい単語やパスワードの検索を示す可能性のある正規表現（たとえば，パスワード，pwd，ログイン，セキュリティ，資格など）を監視します．	**6** **関連大** （検出）
					情報の重要度に応じてネットワークを分割しておくことで不正アクセスの可能性を低減します．また，定期的にアクセスしないアーカイブデータ等への切り離すことで，リスクを低減できます．	14.1-14.3 14.6 14.8 14.9
					管理者権限を含むアカウント管理を適切に実施し，認証情報の漏洩を防ぎます．（平文）ファイルのパスワード保存を禁止する組織ポリシーを確立します．	16 （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
51	6.2	（-3）	内部偵察：資格情報アクセス	ネットワークスニファにより，非暗号化通信で送信される資格情報を収集	デバイスのインベントリを適切に実施します．スニファ用の不正なデバイスの接続を防止します．	1 （防御）
					ホワイトリスト作成ツールを使用し，ネットワークトラフィックを盗聴または分析するために使用される潜在的な悪意のあるソフトウェアを特定・ブロックします．また，許可されたソフトウェアはログを取得します．	2 （防御）
					セキュアなマスターイメージを使用することで非暗号化通信を用いる無許可のサービスの使用を防ぎます．リモート管理はセキュアなチャネルを使用します．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性診断により，非暗号化通信を用いる無許可のサービスの起動を発見できる可能性があります．	3.1-3.2 3.4-3.7 （防御）
					ログの分析により不審な挙動を検出します．スニファで使用されるプロセスを検出します．スニッフィングネットワークトラフィックにつながるイベントを検出します．	**6** **関連大** （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	8.1-8.3 8.6
					ファイアウォールを使用します．また，検証済みのサービスのみの起動を確認します．	9.1-9.4 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					未許可（非暗号通信）プロトコルを通過させないようにすることでリスクを低減します．	11.1-11.3

					Kerberos, SSL, および多要素認証を使用します. ネットワークインフラの構成管理は, 業務ネットワークとは異なる管理用のセグメントを通じて実施します.	11.5 11.6 14.4 16.5 （防御）
					スニッフィングネットワークトラフィックにつながるイベントを検出します. IDS等では非暗号通信プロトコルの使用を検出できます. 非暗号通信が未許可の場合, 使用を停止させます.	12.6-12.7 （検出）
					すべてのワイヤレストラフィックを適切に暗号化します. 無線デバイスに強力な暗号の使用等のセキュアな設定を施します.	15.1-15.5 15.7 15.8 （防御）
					認証情報を送信する際は暗号化チャネルを使用します.	16.5 （防御）
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
52	6.3	(-3)	内部偵察: 資格情報アクセス	アカウントへのアクセスのため, 総当たり攻撃を使用	強固な認証情報を使用します.	**4** **関連大** 11.5 12.11 15.8 （防御）
					有効なアカウントのシステムおよびアプリケーションのログイン失敗の認証ログを監視します. パスワードスプレーの試行に起因する可能性があるさまざまなアカウントでの認証に失敗した回数を監視します.	**6** **関連大** （検出）
					ネットワークデバイスへの総当たり攻撃を検出します.	12.5-12.8
					アカウントの管理を適切に実施します. 特定の回数のログイン試行失敗後にアカウントロックアウトポリシーを設定し, パスワードが推測されないようにします. マルチファクタ認証を使用します.	16.1-16.3 16.6-16.10 16.12 16.13 （防御）
					WAFの導入によりWebアプリケーションへの総当たり攻撃を防御することができます.	18.10 （防御）
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
53	6.4	(-3)	内部偵察: 資格情報アクセス	アクセス権限を持った攻撃者が攻撃に使用するアカウントを作成	サーバ及びクライアントのセキュアな設定を確立します. アクセス制御を設定して, DC等のシステムへのアクセスを制限します. ドメイン管理者アカウントの使用を制限します.	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性診断により, アクセス制限の設定不備を発見できる可能性があります.	3.1-3.2 3.4-3.7 （防御）
					管理者権限の適切な管理により防ぐことができます. マルチファクタ認証を使用します. 管理者権限のアクセスを監視します.	**4.3 4.5 4.9** **関連大** （防御）
					ログ分析により攻撃を検出できる可能性があります. システムおよびドメイン上のアカウントオブジェクトの変更に関連するイベントを収集します. 他の疑わしいアクティビティとの関連でアカウントを変更するかどうかを監視します. 珍しい時間にシステムやサービスに資格情報の異常な使用を監査します.	**6** **関連大** （検出）
					ファイアウォールを設定して, DC等のシステムへのアクセスを制限します.	9.4-9.5 11.1-11.3 （防御）
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
54	6.5	(-3)	内部偵察: 資格情報アクセス	端末に保存されている秘密鍵にアクセス	セキュアな設定により秘密鍵へのアクセスを防ぎます. 重要な秘密鍵を含むフォルダにアクセス許可が適切に設定されていることを確認します.	5.1-5.2 5.4-5.5 （防御）
					継続的な診断により, 設定の不備（アクセス制限）を検出し, 修正することができます.	3.1-3.2 3.4-3.7 （防御）
					管理者権限の適切な管理により防ぐことができます. マルチファクタ認証を使用します. 管理者権限のアクセスを監視します.	**4** **関連大** （防御）
					暗号鍵および証明書に関連するファイルおよびディレクトリへのアクセスを監視し, 異常なアクティビティを探索します.	**6** **関連大** （検出）
					データのアセスメントにより暗号化および完全性コントロールを適用する必要がある機密情報を特定し, ローカルシステムではなく別の暗号ハードウェアに鍵を保管します.	13 （防御）
					秘密鍵に強いパスフレーズを使用します. クリティカルなリソースへのアクセスを許可されたキーとアクセスリストを定期的に監査します.	14.9
					秘密鍵にアクセス可能な管理者権限アカウントの管理を適切に実施します. 特定の回数のログイン試行失敗後にアカウントロックアウトポリシーを設定し, パスワードが推測されないようにします. マルチファクタ認証を使用します.	16
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 （反応）

					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
55	6.6	(-3)	内部偵察: 発見	レジストリにアクセスし, システム情報またはインストールされているソフトウェアの情報を発見	ソフトウェアの棚卸しを実施し, 適切に管理します. ホワイトリストツールを使用して, 情報収集のために使用される不要なシステムユーティリティまたは潜在的に悪意のあるソフトウェアを特定します. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審な操作を検出できる可能性があります.	2 (防御)
					ユーザーが特定のレジストリへアクセスできないようにすることで悪意のある発見を防ぐことが可能です. このため, レジストリへのアクセス制限を適切に実施するため, ソフトウェアにセキュアな設定を施す必要があります.	5.1-5.2 5.4-5.5 (防御)
					設定の不備(アクセス制御設定の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	3.1-3.2 3.4-3.7 (防御)
					レジストリ等の変更が実施可能な管理権限による作業を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また, 管理者権限の悪用を制限する必要があります.	**4** **関連大** (防御)
					OSで収集された監査ログの分析により, 不審なレジストリへのアクセスを検出できる可能性があります. 取得した情報に基づいて他のアクティビティにつながる一連の動作の一部として表示・分析します. システム情報を収集するために必要なアクションのプロセスとコマンドライン引数を監視します.	**6** **関連大** (検出)
					レジストリ情報にアクセス可能な管理者権限を含むアカウントの悪用を制限します. このため, 適切なアカウントの監視, コントロールが必要です.	16 (防御)
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
56	6.7	(-3)	内部偵察: 発見	追加攻撃またはシステム環境の詳細を知るため, 端末に接続されている周辺機器を発見	デバイスのインベントリを適切に実施します. 無許可の野良デバイスは攻撃者に悪用される可能性があります.	1 (防御)
					ソフトウェアの棚卸しを実施し, 適切に管理します. ホワイトリストツールを使用して不要なシステムユーティリティまたは潜在的に悪意のあるソフトウェアを特定します. 各OSタイプに対応したソフトウェアインベントリツールを利用・分析することで不審な操作を検出	2 (防御)
					端末に接続されている周辺機器等の情報にアクセスできないようにすることで悪意のある発見を防ぐことが可能です. レジストリやコントロールパネルへのアクセス制限を適切に実施するため, ソフトウェアにセキュアな設定を施す必要があります.	5.1-5.2 5.4-5.5 (防御)
					設定の不備(アクセス制御設定の不備等)によるシステムの脆弱性は継続的な脆弱性診断によって検出可能です.	3.1-3.2 3.4-3.7 (防御)
					レジストリ等の変更が実施可能な管理権限による作業を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また, 管理者権限の悪用を制限する必要があります.	**4** **関連大** (防御)
					ログ分析により不審なアクセスを検出できる可能性があります. 取得した情報に基づいて他のアクティビティにつながる一連の動作の一部として表示・分析します. ネットワークの情報を収集するために必要なアクションのプロセスとコマンドライン引数を監視しま	**6** **関連大** (検出)
					ファイアウォールを使用します. また, 検証済みのサービスのみの起動を確認します. NICを介して接続された他機器へ悪用可能なサービスを制限します.	9 (防御)
					未許可プロトコルのトラフィックを通過させないようにすることでリスクを低減します. NICを介して接続された他機器へ悪用を制限します.	11.1-11.3
					IDS・IPSによりポートスキャン等でネットワークプリンタなどの周辺機器を特定, 悪用されるリスクを低減します.	12.6 12.7
					無許可の無線LANを発見します. 無許可のBluetoothを使用した周辺機器を無効化しておくことでリスクを低減します.	15.1 15.3 15.4 15.9
					周辺機器を確認可能な管理者権限を含むアカウントの悪用を制限します. このため, 適切なアカウントの監視, コントロールが必要です.	16 (防御)
					攻撃が発覚した場合は, 適切なインシデント対応の実施が必要になります.	19 (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
		(-4)	侵入拡大	(参考)	機器の設定ミス, 管理者権限の不正利用, マルウェアの利用, 不適切なネットワーク分割によりシステムの侵害されるため, 適切な管理が望まれます.	3 5 8 14 (防御)
					継続的な脆弱性診断により, 設定ミス等の悪用可能なシステムの脆弱性を検出できます. また, 侵入拡大を目的とするマルウェアの検出や管理者権限を含む不正なアカウント利用の兆候は検出することができます.	4 8 16 (検出)
					システムに脆弱性が発見された場合はシステムへの影響を考慮し, 迅速に対応を決定する必要があります. また, 監査ログを分析し, 攻撃への対応が可能となります.	4 6 (反応)
					ソフトウェアの棚卸しを実施し, 適切に管理します. ホワイトリストツールを使用して不要なシステムユーティリティまたは潜在的に悪意のあるソフトウェアを特定し, 監査またはブロックします. また, 許可されたソフトウェアはログを取得します.	2 (防御)

57	7.1	(-4)	侵入拡大	システムの認証の仕組みを悪用し，ネットワーク上の別端末を侵害	セキュアな設定（アクセス制限）により，防御できる場合があります．リモートユーザーのアクセス許可を制限します．セキュアなチャネルを利用することで，悪用のリスクを低減します．	**5.1-5.2 5.4-5.5 関連大** （防御）
					継続的な脆弱性検査により，不要な通信サービスを検出・修正し，攻撃を防ぎます．	**3.1-3.2 3.4-3.7 関連大** （防御）
					適切に管理者権限を使用する必要があります．rootや他の特権アカウントによるSSHによるリモートアクセスを許可しないようにします．リモートログインには，リモートデスクトップゲートウェイとマルチファクタ認証を使用します．	**4 関連大** （防御）
					監査ログの分析により不審な挙動を検出できます．認証ログを収集し，異常なアクセスパターン，アクティビティおよび通常の営業時間外のアクセスを分析します．ログインに使用されるアカウントの適切なロギングがオンになっており，一元的に収集します．リモートログイン後に発生するアクセスパターンやアクティビティなどのその他の要因によって，RDPで疑わしい動作や悪意のある動作を検出します．	**6 関連大** （検出）
					不要なサービスを無効化します．不要な場合はRDPサービスを無効にし，Remote Desktop Usersグループから不要なアカウントとグループを削除します．ファイアウォールルールを有効にしてネットワークセキュリティゾーン間のRDPトラフィックをブロックします．	9 （防御）
					ネットワーク機器のセキュアな設定を維持し，二要素認証および暗号化されたセッションを使用してネットワーク機器を管理します．ネットワークインフラの構成管理は，業務ネットワークとは異なる管理用のセグメントを通じて実施することで認証情報の漏洩を防ぎます．リモートログインには，リモートデスクトップゲートウェイとマルチファクタ認証を使用します．	11.1-11.3 11.5 11.6 （防御）
					ネットワーク境界を流れる不審な通信を分析します．Windowsリモート管理などのサービスを無効またはブロックリモートサービスアカウントに強力な2要素認証または多要素認証を使用し，盗まれた資格情報を活用する攻撃者の能力を軽減を図ります．2要素認証傍受テクニックに注意が必要です．リモートログインには，リモートデスクトップゲートウェイとマルチファクタ認証を使用します．	12.6-12.8 12.11 （検出）
					ネットワークを分割することにより，システム全体への感染拡大のリスクを低減します．	**14.1-14.3 関連大**
					無線アクセス経由による認証情報の漏洩を防止するため，適切な無線アクセスコントロールが望まれます．認証プロトコルを適切に実施するため，セキュアな設定を維持します．	15.8 （防御）
					認証情報の悪用を防止するため，適切なアカウント管理が望まれます．システムでローカル管理者アカウントのパスワードを再利用しない．パスワードの解析及び推測されないようにパスワードの複雑さと一意性を確保します．通常はアクセスしないシステムにログインしたユーザアカウントを監視します．	**16 関連大** （防御）
					エンドユーザにユーザ名，パスワードを推測可能なエラーメッセージを表示しないようにすることでリスクを低減できます．	18.7 18.11
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					より短いタイムアウトセッションと，単一のセッションをアクティブにできる最大時間を定義 SSH鍵ペアが強力なパスワードを持っていることを確認	その他 （防御）
58	7.2	(-4)	侵入拡大	リムーバブルメディアの自動実行機能を悪用し，クローズドシステム等にマルウェアを拡散	デバイスのインベントリを適切に実施します．リムーバブルメディアが業務上必要でない場合は，組織ポリシーレベルでそのメディアを許可しないことが重要です．	1.1-1.2 1.4-1.6 （防御）
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアなセキュリティ設定を反映します．不要な場合は自動実行を無効にします．	**5.1-5.2 5.4-5.5 関連大** （防御）
					継続的な脆弱性検査により，セキュリティ設定の不備(自動実行機能等)を検出・修正し，攻撃を防ぎます．	**3.1-3.2 3.4-3.7 関連大** （防御）
					ログの分析により不審な挙動を検出します．リムーバブルメディア上のファイルアクセスを監視しマウント中に実行されるプロセスを検出します．マウント後，またはユーザーが起動したときにリムーバブルメディアから実行されるプロセスを検出します．	**6 関連大** （検出）
					攻撃者がマルウェアを利用する場合，マルウェア対策が有効です． 自動実行機能を無効にし，リアルタイムスキャンを有効にします．	**8.1-8.6 関連大** （防御）
					クローズネットワークのファイアウォール設定のベストプラクティスに従って，ネットワークに出入りするために必要なポートとトラフィックだけを許可します．	9.1-9.4 11.1-11.3 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					シグネチャを使用するネットワーク侵入検知および防止システムを使用して，マルウェア拡散のためのネットワークレベルでのアクティビティを軽減します．	12.6-12.7 （検出）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7

59	7.3	(-4)	侵入拡大	ソフトウェアの脆弱性を突きリモートシステム上でコマンドやバイナリを実行し，システム侵害を拡大	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアなセキュリティ設定を反映します．セキュアなイメージを使用し，脆弱性を残さないようにします．	**5.1-5.2 5.4-5.5 関連大** （防御）
					継続的な脆弱性診断によりパッチが未適用な機器を検出，修正します．脆弱性社内のエンドポイントとサーバーにパッチ管理を採用し，ソフトウェアを定期的に更新します．	**3.1-3.2 3.4-3.7 関連大** （防御）
					ログを分析することで攻撃を検出できる可能性があります．ソフトウェアの悪用により生成されたクラッシュした場合，ソフトウェアおよびOSのクラッシュレポートを参照します．追加のプロセスの起動やファイルへの読み書きなど，特定のプロセスには珍しい動作を検知します．	**6 関連大** （検出）
					古いブラウザ等は脆弱性による悪意のあるコードを実行する可能性があります．サポートされたブラウザによりパッチの適用によりリスクを低減します．	7.1
					マルウェア対策が有効です．サンドボックス化，仮想化およびMicrosoft Enhanced Mitigation Experience Toolkitなどの悪用防止ツールを使用し，発見されていない脆弱性またはパッチが適用されていない脆弱性を悪用して運用を進めるのを困難にします．	**8.1-8.3 8.6 関連大** （防御）
					ネットワークのファイアウォール設定のベストプラクティスに従って，ネットワークに出入りするために必要なポートとトラフィックだけを許可します．	9.1-9.4 11.1-11.3 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					プロキシを強制します．DNSなどのサービスに専用のプロキシを使用し，それぞれのポート/プロトコルを介して通信します．シグネチャを使用するネットワーク侵入検知および防止システムを使用して，ネットワークレベルでのアクティビティを軽減します．	12.6-12.7 12.10 （検出）
					ネットワークを分割することにより，システム全体への感染拡大のリスクを低減します．	**14.1-14.3 関連大**
					無許可の無線アクセスポイント経由での侵害を防ぎます．ピアツーピア無線ネットワーク機能を悪用し，侵害の拡大のリスクを低減します．	15.1-15.6
					SQLインジェクションによるWebアプリケーションの脆弱性の悪用等で任意のコマンドが実行される可能性があります．WAFや脆弱性診断による脆弱性修正により攻撃を防ぎます．	18.1-18.4 18.6-18.8 18.10 18.11 （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
60	7.4	(-4)	侵入拡大	標的が使用するOSやアプリケーションの機能・仕組みを悪用し，システム侵害を拡大	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリスト作成ツールを使用し，ログオンスクリプトの変更によって実行される可能性のある悪質なソフトウェアを特定し，ブロックします．また，使用が許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアな設定（アクセス制限等）を施し，管理権限が必要な機能の悪用を制限します．ログオンスクリプトへの書き込みアクセスを特定の管理者に制限します．	**5.1-5.2 5.4-5.5 関連大** （防御）
					継続的な脆弱性診断により，適切な設定（アクセス制限等）を確認・修正し，悪用を制限します．	**3.1-3.2 3.4-3.7 関連大** （防御）
					PowerShell実行ポリシーを管理者に制限し，署名付きスクリプトのみの実行を許可します．このため，管理者権限の悪用を防止する必要があります．アカウントの監視により，不正なアカウント利用を防ぎます．許可された管理者だけにアプリケーション導入システムへのアクセスを許可します．開発システムにアクセスするために使用されるアカウントの資格情報が一意であり，企業ネットワーク全体で使用されていないことを確認します．グループポリシーおよびマルチファクタ認証を使用します．アカウント特権を分離します．	**4 16 関連大** （防御）
					監査ログの収集・監視により検出できる可能性があります．異常なユーザーまたは異常なアクセスのログオンスクリプトを監視（通常の管理業務の外で異常なアカウントによって追加または変更されたファイルを監視）します．ソフトウェアの展開ログを監査し，不審な活動や不正な活動を検出します．	**6 関連大** （検出）
					マイクロソフトの強化された緩和エクスペリエンスツールキット（EMET）やアタックサーフェスリダクション（ASR）機能といったマルウェア対策を施します．	**8.1-8.3 8.6 関連大** （防御）
					ポート，プロトコル，サービスを検証，不要なサービス等はブロック，定期的な確認を実施し，リスクを低減できます．ファイアウォールの使用します．グループポリシーおよびマルチファクタ認証を使用します．	9 11 （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					境界ネットワークに配置したセキュリティ機器により，OSやアプリケーションの機能・仕組みを悪用した不審な通信を検知・防御します．	12.6-12.7 （検出）
					グループポリシーおよびマルチファクタ認証を使用し，重要なネットワークシステムの適切なシステムとアクセス分離を確保します．	**14.1-14.3 関連大**
					不要な無線アクセス機能を無効化し，悪用を防ぎます．BYODのような信頼できないネットワーク経由でシステム侵害を拡大されるのを防ぎます．	15.4-15.5 15.10 （防御）

					外部に公開しているアプリケーションの適切な管理が望まれます．悪意のあるコードが実行されないようにWAFやセキュリティ設定により防御します．	18.1-18.4 18.6-18.8 18.10 18.11 （防御）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
	8	（-4）	持続性確立	（参考）	持続性を確立にはマルウェアを用いることが想定されます．このため，対策にはマルウェア対策が有効な場合が多いと考えられます．	8 （防御） （検出）
61	8.1	（-4）	持続性確立	悪意のあるファイルに隠れファイル・ディレクトリ属性を付与し，利用者から隠蔽	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用して，悪質なソフトウェアを特定しブロックします．許可されたソフトウェアはログを取得します．使用が許可されたソフトウェアはログを収集します．	2 （防御）
					監査ログの分析により検出できる可能性があります．先頭に”．”を付けて作成するファイルのファイルシステムとシェルコマンドを監視します．attrib.exeのWindowsコマンドラインを使用して隠し属性の追加を監視します．	6 （検出）
					メール経由で，悪意のあるファイルの流入を阻止します．	7.9-7.10
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.3 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
62	8.2	（-4）	持続性確立	既存のファイルやレジストリ情報を変更し，悪意のあるプログラムやスクリプトを継続的に実行	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，実行キーまたはスタートアップフォルダの持続性によって実行される潜在的な悪意のあるソフトウェアを特定し，ブロックします．また，許可されたソフトウェアはログを取得します．	2 （防御）
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．レジストリハイブに適切なアクセス許可が設定されていることを確認します．ユーザーアカウントとグループの権限を制限します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備を検出・修復します．ファイルシステムのアクセス許可を検出できる監査ツールを使用します．	3.1-3.2 3.6-3.7 （防御）
					管理権限を使用したソフトウェアによる実行可能な処理を最小限に抑えます．必要な場合にのみ管理アカウントを使用を許可します．また，管理者権限の悪用を制限する必要があります．アカウントの監視により，不正な監視者アカウントの利用を防ぎます．	4 16 （防御）
					監査ログの分析により不審な挙動を検出できます．既知のソフトウェア，パッチサイクル等と相関のないキー実行のためのレジストリ変更を監視します．コマンド制御のためのネットワーク接続などの他のアクティビティにつながる一連の動作の一部として検出します．	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.4 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します．	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					Autorunsなどのツールを使用し，実行キーのレジストリの場所とスタートアップフォルダを一覧表示します．	その他 （検出）
63	8.3	（-4）	持続性確立	OSの起動時に動作するプロセス・スクリプト一覧に悪意のあるプログラム・スクリプトを追加	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，悪意のあるソフトウェアを特定し，ブロックします．また，許可されたソフトウェアはログを取得します．	2 （防御）
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります．起動時に動作するプロセスが保存されているディレクトリに適切なアクセス許可が設定されていることを確認します．すべてのユーザーが/Library/StartupItemsディレクトリに書き込むことを禁止し，起動項目の登録ができないようにします．特定のユーザーだけがスタートアップ項目を編集し，権限の昇格に活用できないように適切な権限を適用します．	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備（アクセス制御）を検出・修復します．	3.1-3.2 3.6-3.7 （防御）
					管理権限を使用したソフトウェアによる実行可能な処理を最小限に抑えます．必要な場合にのみ管理アカウントを使用を許可します．また，管理者権限の悪用を制限する必要があります．アカウントの監視により，不正な監視者アカウントの利用を防ぎます．	4 16 （防御）
					監査ログの分析により不審な挙動を検出できます．Library/StartupItemsフォルダの変更を監視します．ホワイトリストに照らしてチェック．ブートアッププロセス中に実行されるプロセスを監視し，異常なアプリケーションや不明なアプリケーションの動作をチェックします．	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	**8.1-8.4 8.6 関連大** （防御）

					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
64	8.4	（-4）	持続性確立	OSやアプリケーションの設定を変更し，システムアクセスへの永続性を確保	ソフトウェアの棚卸しを実施し，適切に管理します. ホワイトリストツールを使用し，悪意のあるソフトウェアを特定し，ブロックします. また，許可されたソフトウェアはログを取得します.	2 （防御）
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります. 許可されたユーザのみがOSやアプリケーションの設定を変更できるようにします.	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定（アクセス制御）の不備を検出・修復します.	3.1-3.2 3.6-3.7 （防御）
					管理権限を使用したソフトウェアによる実行可能な処理を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また，管理者権限の悪用を制限する必要があります. アカウントの監視により，不正な監視者アカウントの利用を防ぎます.	4 16 （防御）
					監査ログの分析により不審な挙動を検出できる可能性があります. 未知のプロセス起動アクティビティまたはそのプロセスの通常ではないファイルタイプとの関連付けを実施します. 他のテクニックに関連する可能性のある他のコマンドを実行するためのプロセスコールツリーの異常を調査します.	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です.	**8.1-8.4 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
65	8.5	（-4）	持続性確立	OSの下層で動作するブートキットを悪用して，永続的にシステムにアクセス	ソフトウェアの棚卸しを実施し，適切に管理します. ホワイトリストツールを使用し，悪意のあるソフトウェアを特定し，ブロックします. また，許可されたソフトウェアはログを取得します.	2
					セキュアな設定（アクセス制限）の付与により防御ができる可能性があります. 許可されたユーザのみがOSの設定を変更できるようにします. MBRとVBRの整合性チェックを実行します. MBR（マスター・ブート・レコード）とVBR（ボリューム・ブート・レコード）のスナップショットを撮り，既知の良いサンプルと比較します.	5.1-5.2 5.4-5.5 （防御）
					脆弱性診断により設定の不備（アクセス制御）を検出・修復します. OSやアプリケーションを最新にし，ブートキットマルウェアの感染を防止します.	3.1-3.2 3.6-3.7 （防御）
					この操作を実行するために必要な特権アカウントへの攻撃者によるアクセスを防ぐため，適切なアクセス権があることを確認します. 管理権限を使用したソフトウェアによる実行可能な処理を最小限に抑えます. 必要な場合にのみ管理アカウントを使用を許可します. また，管理者権限の悪用を制限する必要があります. アカウントの監視により，不正な監視者アカウントの利用を防ぎます.	4 16 （防御）
					ブートキットマルウェア感染に別のマルウェアを使用する場合，マルウェア対策が有効です.	**8.1-8.3 8.6 関連大** （防御）
					マルウェア感染からの修復にはバックアップからデータを修復します.	10 （復旧）
					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります.	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
66	8.6	（-4）	持続性確立	リモートサービスを使用して持続的にネットワークにアクセス	セキュアな設定（アクセス制限）により，防御できる場合があります. リモートユーザーのアクセス許可を制限します. セキュアなチャネルを利用することで，悪用のリスクを低減します.	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性検査により，不要なリモートサービスを検出・修正し，攻撃を防ぎます.	3.1-3.2 3.6-3.7 （防御）
					リモートサービスに使用するアカウントの管理を適切に実施します. アカウントの監視により，不正な管理者アカウントの利用を防ぎます.	4 16 （防御）
					監査ログの分析により不審な挙動を検出できます. 認証ログを収集し，異常なアクセスパターン，アクティビティおよび通常の営業時間外のアクセスを分析します.	6 （検出）
					マルウェアがリモートサービスを悪用する場合，マルウェア対策が有効です.	**8.1-8.3 8.6 関連大** （防御）
					ネットワークのファイアウォール設定のベストプラクティスに従って，ネットワークに出入りするために必要なポートとトラフィックだけを許可します. ネットワークプロキシ，ゲートウェイ，ファイアウォールを使用し，内部システムへの直接リモートアクセスを拒否します.	9 11.1-11.3 11.5-11.7 （防御）
					ネットワークプロキシ，ゲートウェイ，ファイアウォールを使用し，内部システムへの直接リモートアクセスを拒否します. また，ネットワーク境界を流れる不審な通信を分析します. Windowsリモート管理などのサービスを無効またはブロックリモートサービスアカウントに強力な2要素認証または多要素認証を使用し，盗まれた資格情報を活用する攻撃者の能力を軽減を図ります. 2要素認証傍受テクニックに注意が必要です.	12.6-12.7 （検出）

					攻撃が発覚した場合は，適切なインシデント対応の実施が必要になります．	19 （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					VPN等管理対象のリモートアクセスシステムの集中管理対象のコンセントレータを介してリモートサービスへのアクセスを制限します．	その他 （防御）
		(-5)	任務目的実行	（参考）	攻撃者の目的は改ざん，サービスの無効化，情報窃取等が考えられrます．データを攻撃前の状態に戻すためにデータ復旧能力が必要になります．	10 （復旧）
					攻撃者の目的は改ざん，サービスの無効化，情報窃取等が考えられrます．データを攻撃者から守るためにデータ保護が必要になります．	13 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	19 （反応）
67	9.1	(-5)	任務目的実行：収集	標的で使用可能なAPIにより音声やクリップボード，スクリーンキャプチャなどの情報を収集	デバイスのインベントリを適切に実施します．音声及び映像等が外部デバイス経由で収集されるのを防ぎます．	1 （防御）
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用して，オーディオを記録するために使用される可能性のある悪質なソフトウェアを特定しブロックします．許可されたソフトウェアはログを取得します．	2 （防御）
					セキュアな設定（アクセス制限）により，防御できる場合があります．不必要なAPI機能のアクセスを制限します．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性検査により，不要なAPI機能を修正し，攻撃を防ぎます．	3.1-3.2 3.6-3.7 （防御）
					ログを分析することで不審な挙動を検知できる可能性があります．録音等APIにアクセスする不明なプロセスや異常なプロセスおよびオーディオデータを含むファイルをディスクに定期的に書き込むプロセスを検知します．他の疑わしい活動や非ユーザ主導の活動との相関により検知します．	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	8.1-8.3 8.6 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
68	9.2	(-5)	任務目的実行：収集	標的の内部情報を効率よく収集するために自動化技術を活用	ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用し，不要なシステムユーティリティ，サードパーティツールまたは潜在的に悪意のあるソフトウェアを特定しファイルの監査やブロックします．また，許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアな設定（アクセス制限）により，防御できる場合があります．機密情報へのアクセスを制限します．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性検査により，アクセス制限設定の不備を修正し，攻撃を防ぎます．	3.1-3.2 3.6-3.7 （防御）
					ログを分析することで不審な挙動を検知できる可能性があります．連続的なファイルの起動を実行し，ファイルシステム上の別の場所に一度に多くのファイルをコピーする異常なプロセスを実行するファイルアクセスの監視します．	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	8.1-8.3 8.6-8.8 （防御）
					外部から内部ネットワークの情報収集をされる場合があります．不要なサービスを無効化しておくことで自動化ツール（スキャナ）によるリスクを低減します．	9 （防御）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					ネットワークに出入りするために必要なポートとトラフィックだけを許可します．自動化ツール（スキャナ）によるリスクを低減します．	11.1-11.3
					ネットワーク内の情報収集時に自動化ツールを使用する場合，特異な通信の発生により，IDSで検知できる場合があります．また，境界で不審な通信（IP・ポート）を遮断し，通過する通信パケットを収集することでリスクを低減します．	12.1-12.7
					機密データの保護のため，機密情報の暗号化とシステム外の保管を実施します．	**13** **関連大**
					データの重要度に応じて，ネットワークを分離する必要があります．ファイルへのACLの設定やVLANの使用によりリスクを低減します．機密データがアクセスされた場合，ログを取得します．	14.1-14.3 14.5-14.9 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					デバイスのインベントリを適切に実施します．無許可のリムーバブルメディア経由で情報を収集されるのを防ぎます．	1 （防御）
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールを使用して不要なシステムユーティリティまたは潜在的に悪意のあるソフトウェアを検出し，ブロックします．また，許可されたソフトウェアはログを収集します．	2 （防御）
					ファイルにアクセス制御を施します．OS等のセキュアな設定により，攻撃を防ぎます．	5.1-5.2 5.4-5.5 （防御）

69	9.3	(−5)	任務目的実行：収集	標的内のローカルドライブ・リモートドライブ・リムーバブルメディアから情報を収集	継続的な脆弱性検査により，セキュリティ設定の不備を検出・修正し，攻撃を防ぎます．	3.1−3.2 3.6−3.7 （防御）
					ログを分析することで不審な挙動を検知できる可能性があります．システムに接続されたリムーバブルメディアからファイルを収集するためのアクションのプロセスとコマンドライン引数を監視します．	6 （検出）
					マルウェアを使用する場合，マルウェア対策が有効です．	8 （防御）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					機密データの保護のため，機密情報への暗号化により標的の物理的なアクセスから情報を収集されるのを防ぎます．	**13** **関連大** （防御）
					データの重要度に応じて，ネットワークを分離する必要があります．ファイルへのACLの設定やVLANの使用によりリスクを低減します．機密データがアクセスされた場合，ログを取得します．	14.1−14.3 14.5−14.9 （防御）
					攻撃が物理的に侵入し，システムにアクセスする場合があります．無人のワークステーションにはスクリーンロックを設定することで，リスクを低減します．	16.11 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1−20.3 20.5−20.7
70	9.4	(−5)	任務目的実行：情報流出	データの暗号化・圧縮・転送サイズ制限を行い，標的に気づかれないように情報を取得	デバイスのインベントリを適切に実施します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2 （防御）
					ログの分析により，不審な通信を検出できる可能性があります．一般的でないデータフロー（例えば，クライアントがサーバから受信するデータよりもかなり多くのデータを送信する）を分析します．プロセスが一定サイズのデータパケットを一貫して送信する長い接続を維持している場合やプロセスが一定の間隔で接続を開いて固定サイズのデータパケットを送信している場合は集約データ転送を行っている可能性があります．既知の暗号化等のユーティリティのコマンドライン引数のプロセス監視によって検出します．	6 （防御）
					マルウェアを使用している場合，マルウェア対策が有効です．	8.1−8.3 8.6−8.8 （防御）
					外部から内部ネットワークの情報収集をされる場合があります．悪用される可能性がある不要なサービスを無効化しておく必要があります．	9.1−9.4 （防御）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					ネットワークに出入りするために必要な通信だけの通過を許可し，リスクを低減します．	11.1−11.3
					シグネチャを使用するネットワーク侵入検知および防止システムを使用して，ネットワークレベルでのアクティビティを軽減します．ファイルヘッダーを分析するネットワーク侵入検出またはデータ損失防止システムを使用し，圧縮ファイルの通過を検出します．	12.1−12.7 （防御）
					データのアセスメントにより機密情報を特定し，適切な対策を施し，リスクを低減します．	**13** **関連大** （防御）
					データの重要度に応じて，ネットワークを分離する必要があります．ファイルへのACLの設定やVLANの使用によりリスクを低減します．機密データがアクセスされた場合，ログを取得します．	14.1−14.3 14.5−14.9 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1−20.3 20.5−20.7
71	9.5	(−5)	任務目的実行：情報流出	任意の通信プロトコルを使用し，情報を収集	継続的な脆弱性検査により，不要な通信サービスを検出・修正し，攻撃を防ぎます．	3.1−3.2 3.6−3.7 （防御）
					境界ネットワーク上を通過する通信ログを分析します．異常なデータフローについてネットワークデータを分析します．これまでに見たことがないネットワークを利用するプロセスは疑わしいです．パケットの内容を分析して，使用されているポートの予想されるプロトコル動作に従わない通信を検出します．	6 （検出）
					マルウェアを使用している場合，マルウェア対策が有効です．	8.1−8.3 8.6−8.8 （防御）
					許可されたポート等のみが起動してることを確認します．不要なサービスは無効化することでリスクを低減します．	9.1−9.4 （防御）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					ネットワークのファイアウォール設定のベストプラクティスに従って，ネットワークに出入りするために必要なポートとトラフィックだけを許可します．	11.1−11.3 （防御）
					プロキシを強制し，DNSなどのサービスに専用のプロキシを使用し，それぞれのポート/プロトコルを介して通信します．シグネチャを使用するネットワーク侵入検知および防止システムを使用して，ネットワークレベルでのアクティビティを軽減します．	12.1−12.10 （防御）
					データのアセスメントにより機密情報を特定し，適切な対策を施し，リスクを低減します．	**13** **関連大** （防御）

					データの重要度に応じて，ネットワークを分離する必要があります．ファイルへのACLの設定やVLANの使用によりリスクを低減します．機密データがアクセスされた場合，ログを取得します．	14.1-14.3 14.5-14.9 （防御）
					SQLインジェクションによるWebアプリケーションの脆弱性の悪用等で情報が流出する可能性があります．WAFや脆弱性診断による脆弱性修正により攻撃を防ぎます．	18.1-18.8 18.10 18.11 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
72	9.6	（-5）	任務目的実行：情報流出	外部デバイス，携帯電話，MP3プレイヤーなどを使用し，情報を収集	デバイスのインベントリを適切に実施します．リムーバブルメディアが業務上必要でない場合は，組織ポリシーレベルでそのメディアを許可しないことが重要です．	1 （防御）
					セキュアな設定（アクセス制限，自動実行機能の無効化）により，防御できる場合があります．機密情報へのアクセスを制限します．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性検査により，アクセス制限設定等の不備を修正し，攻撃を防ぎます．	3.1-3.2 3.6-3.7 （防御）
					ログの分析により不審な挙動を検出します．リムーバブルメディア上のファイルアクセスを監視しマウント中に実行されるプロセスを検出します．	6 （検出）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					機密データの保護のため，機密情報への暗号化により標的の物理的なアクセスから情報を収集されるのを防ぎます．	**13** **関連大** （防御）
					データの重要度に応じて，ネットワークを分離する必要があります．ファイルへのACLの設定やVLANの使用によりリスクを低減します．機密データがアクセスされた場合，ログを取得します．	14.1-14.3 14.5-14.9 （防御）
					BluetoothやBYODシステム経由で情報収集されるリスクを防ぐため，不要な機能を無効化します．	15.4-15.6 15.9 （防御）
					攻撃が物理的に侵入し，システムにアクセスする場合があります．無人のワークステーションにはスクリーンロックを設定することで，リスクを低減します．	16.11 （防御）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
73	9.7	（-5）	任務目的実行：遠隔操作	リムーバブルメディアによりクローズネットワークのホストを侵害し，コマンド及び制御トラフィックを実行	デバイスのインベントリを適切に実施します．リムーバブルメディアが業務上必要でない場合は，組織ポリシーレベルでそのメディアを許可しないことが重要です．	1 （防御）
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2 （防御）
					セキュアなセキュリティ設定を反映します．不要な場合は自動実行を無効にします．	5.1-5.2 5.4-5.5 （防御）
					継続的な脆弱性検査により，セキュリティ設定の不備(自動実行機能等)を検出・修正し，攻撃を防ぎます．	3.1-3.2 3.6-3.7 （防御）
					ログの分析により不審な挙動を検出します．リムーバブルメディア上のファイルアクセスを監視しマウント中に実行されるプロセスを検出します．	6 （検出）
					攻撃者がマルウェアを利用する場合，マルウェア対策が有効です．	8 （防御）
					許可されたポート等のみが起動してることを確認します．不要なサービスは無効化することでリスクを低減します．	9.1-9.4 （防御）
					攻撃を受けたデータは信頼性が著しく低下（改ざんの恐れ）します．この場合，攻撃前の状態にデータを復旧する必要があります．	**10** **関連大** （復旧）
					ネットワークのファイアウォール設定のベストプラクティスに従って，ネットワークに出入りするために必要なポートとトラフィックだけを許可します．	11.1-11.3 （防御）
					シグネチャを使用するネットワーク侵入検知および防止システムを使用して，ネットワークレベルでのアクティビティを軽減します．	12.1-12.7 （検出）
					攻撃が成功した場合は，メディア発表も考慮したインシデント対応の実施が必要になります．	**19** **関連大** （反応）
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．	20.1-20.3 20.5-20.7
					不許可のマルウェア感染した持ち込みPCを接続することで，攻撃者が内部ネットワークに侵入できる可能性があります．デバイスのインベントリを適切に管理し，リスクを低減します．	1 （防御）
					ソフトウェアの棚卸しを実施し，適切に管理します．ホワイトリストツールによる不正なソフトウェアの起動を防止します．また，許可されたソフトウェアはログを収集します．	2
					継続的な脆弱性検査により，不要な通信サービスを検出・修正し，攻撃を防ぎます．	3.1-3.2 3.6-3.7 （防御）

74	9.8	(-5)	任務目的実行:遠隔操作	コンピュータ上の通信ポートを介して,コマンドおよび制御トラフィックを送信	境界ネットワーク上を通過する通信ログを分析します. 異常なデータフローについてネットワークデータを分析します. これまでに見たことがないネットワークを利用するプロセスは疑わしいです. パケットの内容を分析して, 使用されているポートの予想されるプロトコル動作に従わない通信を検出します.	6 (検出)
					攻撃者がマルウェアを利用する場合, マルウェア対策が有効です.	8.1-8.3 8.6-8.8 (防御)
					許可されたポート等のみが起動してることを確認します. 不要なサービスは無効化することでリスクを低減します.	9.1-9.4 (防御)
					攻撃を受けたデータは信頼性が著しく低下(改ざんの恐れ)します. この場合, 攻撃前の状態にデータを復旧する必要があります.	**10** **関連大** (復旧)
					ネットワークのファイアウォール設定のベストプラクティスに従って, ネットワークに出入りするために必要なポートとトラフィックだけを許可します.	11.1-11.3 (防御)
					プロキシを強制し, DNSなどのサービスに専用のプロキシを使用し, それぞれのポート/プロトコルを介して通信します. シグネチャを使用するネットワーク侵入検知および防止システムを使用して, ネットワークレベルでのアクティビティを軽減します.	12.1-12.7 (検出)
					無線ピアツーピア接続により, 制御コードを実行されるリスクを低減します.	15.6
					攻撃が成功した場合は, メディア発表も考慮したインシデント対応の実施が必要になります.	**19** **関連大** (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
75	9.9	(-5)	任務目的実行:遠隔操作	暗号プロトコルまたはアルゴリズムを使用して, コマンドおよび制御トラフィックを隠蔽	ソフトウェアの棚卸しを実施し, 適切に管理します. ホワイトリストツールによる不正なソフトウェアの起動を防止します. また, 許可されたソフトウェアはログを収集します.	2 (防御)
					ログの分析により, 不審な通信を検出できる可能性があります. 暗号化ユーティリティのコマンドライン引数をプロセス監視によって検出します.	6 (防御)
					マルウェアを使用している場合, マルウェア対策が有効です.	8.1-8.3 8.6-8.8 (防御)
					許可されたポート等のみが起動してることを確認します. 不要なサービスは無効化することでリスクを低減します.	9.1-9.4 (防御)
					攻撃を受けたデータは信頼性が著しく低下(改ざんの恐れ)します. この場合, 攻撃前の状態にデータを復旧する必要があります.	**10** **関連大** (復旧)
					ネットワークのファイアウォール設定のベストプラクティスに従って, ネットワークに出入りするために必要なポートとトラフィックだけを許可します.	11.1-11.3 (防御)
					シグネチャを使用するネットワーク侵入検知および防止システムを使用して, ネットワークレベルでのアクティビティを軽減します. これまでに見たことがないネットワークを利用するプロセスは疑わしいです.	12.1-12.7 (防御)
					攻撃が成功した場合は, メディア発表も考慮したインシデント対応の実施が必要になります.	**19** **関連大** (反応)
					ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です.	20.1-20.3 20.5-20.7
					マルウェアが対称鍵でカスタム暗号化を使用する場合, サンプルからアルゴリズムと鍵を取得, デコードし, 解析します.	その他 (検出)