JNSA 2023年度活動報告会

「実はとっても焦っています！ 対策ハンドブックの検討状況」

西日本支部
今すぐ実践できる工場セキュリティ対策のポイント検討WG
岡本　登

何を焦っているのか??

医療関係でランサムウェアによる重大なセキュリティインシデントが発生
2021年10月、徳島県つるぎ町立半田病院
2022年10月、大阪急性期・総合医療センター

他にも
2017年　福島医大病院　検査装置に不具合が発生
2018年　宇陀市立病院　電子カルテ
2021年　市立東大阪医療センター　遠隔読影システム
2022年　春日井リハビリテーション病院　電子カルテ
日本歯科大学付属病院　電子カルテ、会計システム
青山病院　電子カルテ
鳴門山上病院　電子カルテ

次は…

次は工場で大規模な被害??

- セキュリティ環境の観点では医療現場と製造現場は類似点が多い
- これまでも工場のランサムウェア被害は発生しているが、サプライチェーン全体が大きな影響を受ける被害が懸念される。

たとえば、RaaS（Ransomware as a Service）
ランサムウェアを使った攻撃を簡単に行うためのパッケージ提供サービス
RaaSは利用料金を払えば、技術力のない攻撃者でも簡単に攻撃ができる。成果報酬型で提供者と利用者が利益を分配する形態もある

	エリート	プレミアム	スタンダード	テスト
Ranionランサムウェア（32ビット）	○	○	○	○
Ranionランサムウェア（64ビット）	○	○	○	○
復号化ツール	○	○	○	○
サブスクリプション期間（月数）	12	12	6	1
報酬の割合	—	—	—	—
ランサムウェアの機能				
遅延起動	○	○	○	○
遅延暗号化	○	○	○	○
タスクマネージャー	○	○	○	○
レジストリエディタ無効化ツール	○	○	○	○
UAC（ユーザーアカウント制御）の迂回	○	○	○	○
デスクトップの壁紙変更	○	○	○	○
IP追跡	○	○	○	○
オフライン暗号化	○	○	○	—
サポート	○	○	○	—
リアルタイムクライアントマネージャー	○	○	○	—
アドオン：ドロッパー（+90 USD）	○	AUP[1]	AUP	—
アドオン：クローン（+90 USD）	○	AUP	AUP	—
アドオン：FUD+（+300 USD）	○	AUP	AUP	AUP
アドオン：プロセスの強制終了不可（+90 USD）	○	AUP	AUP	—
価格（USD）	1900	900	490	120

米国時間2021年9月30日に掲載されたフォーティネットブログより

狙われるのは
大企業か、それともサプライチェーンの一端を担う中小企業か

ハンドブック３部作

リスクアセスメント編

セキュリティリスクアセスメントを自らの手で実施できる参考書
2022.6 初版公開（https://www.jnsa.org/result/west/2022/index.html）

リ ス ク 対 策 編

今回のご紹介はここ

自社の環境に合ったセキュリティ対策が選択・実行できる参考書
2023.秋 初版公開予定

サイバーBCP策定編

従来の災害対応BCPにセキュリティ観点を加えるための参考書
2024.春 初版公開予定

セキュリティリスク対策編

【検討の観点】

- アセスメント結果とのリンク
- 対策を選ぶ視点（狙う効果、実行者、リードタイム、コストなど）
- 中小企業がすぐに取り組める対策
- 具体的な解説（ただし、製品などは特定しない）
- 対策効果の評価方法

中小企業にとって、コストは最優先の判断基準なのか？
→ この議論で白熱。本当にやらなければならないことにはコストをかけるという意見も
→ では、なぜ対策が進まないのか？
→ やらなければならないという納得感がないから…
→ 危機感が伝わっていない？痛い目に遭わないと実感しない？
→ マルウェア入りのUSBメモリーを近くに捨てておくとか…
（**よい子は絶対にやってはいけません!!**）

AI 話題の生成系AIは優等生

JNSA

脅威の入口		対策（ChatGPT-3.5回答原文のまま）						
		1	2	3	4	5	6	7
0	工場全般	アクセス制御：工場内に立ち入るためのアクセスを制御することが重要です。工場への入り口には、セキュリティゲートを設置し、認証システムを設けることで、不正な立ち入りを防止することができます。	監視システムの設置：工場内に防犯カメラなどの監視システムを設置することで、監視員が隅々まで確認することができます。また、緊急時には一瞬で対応できます。	セキュリティ教育の実施：社員に対して、セキュリティ教育を定期的に実施することで、セキュリティ意識を高めることができます。具体的には、不審者への取り扱い方や、保管場所への注意喚起などが挙げられます。	機器の制限：許可されていない機器は持ち込ませないようにし、社員が使用できる機器には制限を設け、異常なアクセスや利用を警戒することが大切です。	火災・災害対策：工場内には自動火災報知機や自動消火装置、非常用の脱出路などを設置することで、火災や地震、津波などの災害が発生した場合にも迅速に対応できます。	定期的なメンテナンス：監視システムやセキュリティ関連の機器については、常に最新の状態に保つため、定期的なメンテナンスを行い、必要に応じて更新や修理を行うことが重要です。	
1	USBメモリ	USBメモリーの使用を制限する 工場内でのUSBメモリーの使用を制限することにより、マルウェア感染や機密情報の漏洩を防ぐことができます。使用を制限する際には、必要な業務に必要な人物に対して利用可能なUSBメモリーを許可することが必要です。	USBメモリーにパスワードを設定する USBメモリーにパスワードを設定することで、不正なアクセスを防ぐことができます。また、機密情報が保存されたUSBメモリーを紛失した場合でも、パスワード保護されているため情報漏洩のリスクを低減できます。	USBメモリーの譲渡を禁止する USBメモリーの譲渡を禁止することで、情報漏洩のリスクを低減できます。また、不必要なUSBメモリーは破棄することで、不要な情報漏洩リスクを回避することもできます。	USBメモリーの利用記録を取る USBメモリーの利用記録を取ることで、誰がどのようなファイルを使用したかを確認することができます。記録を取ることで、不正なアクセスや情報漏洩が発生した場合に迅速な対処ができるようになります。	マルウェア対策を行う USBメモリーはマルウェアの侵入経路になることがあります。マルウェア対策を徹底することにより、USBメモリーを通じたマルウェア感染を防ぐことができます。また、USBメモリーに保存されたデータを定期的にスキャンすることで、感染の早期発見も可能になります。		
2	持込パソコン	パスワードでアクセスを制限する 持ち込まれたパソコンには、アクセス権限を制限するパスワードを設定することで不正なアクセスを防止できます。また、パスワードは強力なものを使用するようにしましょう。	ネットワークの分離を行う 持ち込まれたパソコンが感染している場合、同じネットワーク内に接続されている他のシステムにも影響が及ぶ可能性があるため、持ち込まれたパソコンとネットワークを分離することが必要です。	ウイルス対策ソフトの導入 ウイルス対策ソフトを事前にインストールしておくことで、持ち込まれたパソコンがウイルスに感染していた場合でも早めに対処できます。	パソコンのログを取る サポート担当者は持ち込まれたパソコンにアクセスし、作業を行うことがあります。パソコンのログを適切に取得し、不正なアクセスがあった場合にすぐに対処できるようにします。作業後にログを削除することも大切です。	コンプライアンスを厳守する 保守作業には、個人情報保護法や特定電子メール法、法人データ保護法などの法律に基づく業務が含まれる場合があります。保守作業前に法令の把握を行い、リスクを回避するように意識しましょう。		
3	スマホ・タブレット	パスワードでアクセスを制限する スマホやタブレットにはアクセス権限を制限するパスワードを設定することで不正なアクセスを防止できます。また、パスワードは強力なものを使用するようにしましょう。	Wi-Fiの利用を制限する 工場内のWi-Fiに接続することで、ウイルス感染や不正アクセスなどのリスクが高まるため、スマホやタブレットでのWi-Fi接続を制限することが重要です。	Bluetoothをオフにする Bluetoothをオフにすることで、スマホやタブレットから不正な接続をされるリスクを低減できます。	ウイルス対策ソフトの導入 ウイルス対策ソフトをスマホやタブレットに導入することで、不正なアクセスやウイルスに感染した場合のリスクを低減できます。	紛失対策を徹底する スマホやタブレットが紛失した場合、情報漏洩のリスクが高まります。そのため、パスコードや指紋認証などで画面ロックをかけ、紛失した場合に遠隔でデータを削除できるアプリを導入することが重要です。	利用規定を策定する スマホやタブレットの利用規定を策定し、業務に必要な情報やアプリ以外はインストールしないように徹底します。また、スマホやタブレットの取り扱い方法についても、徹底した教育を行い、使用者がルールを理解できるようにします。	

これは当たり前の回答。負けられない！我々にはもっと工夫ができるはず！

対策一覧（検討途中）

脅威の入口		対策の種類			対策の分類			費用		
		被害に遭わない	被害を早期発見	被害から早期復旧	物理的	組織・人的	技術的	内部活動	投資小	投資大
USBメモリー	01	01,02,03	A	B	02	01	03	01	02,03	
持込パソコン	02	01,02,03	C	D		01	02,03	01	02,03	
スマホ・タブレット	03	01,02,03	E	F		01	02,03	01	02,03	
IoT機器・センサー	04	01,02,03,04	G	H		01,02	03,04	01,02	03,04	
複合機	05	01,02,03,04	05	I		01,03	02,04,05	01,02,03,05	04	
ハンディターミナル	06	01,02,03	04,05	J	01	01,04,05	02,03	01,02,04,05	03	
OAネットワーク	07	01,02,03,04,05	06,07	K	01	01,02,04,05	03,05,06,07	01,02	03,04,05	06,07
インターネット	08	01,02,03,04,08,09	05,06,09	07	01	01,02,03,04,07,08	04,05,06,09	01,02,03,04,07,08		05,06
WiFi（無線AP）	09	01,02,03,04	L	M		01	02,03,04	01	02,03,04	
保守用ネットワーク	10	01,02,03,04	N	O		01,02,04	03	01,02,03,04		
クラウドサービス	11	01,02,03,04,07	05	06		01,07	02,03,04,05,06	01,02,07	03,04,06	05
部品・原材料	12	P	01,02	03		01,02,03		01,02,03		
新規購入機器	13	01,02	Q	R		01,02		02	01	
共通	#	04,05	01	02,03,06,07		04,05,06,07	01,02,03	04,05,06	02,07	01,03

※最終的な「セキュリティリスク対策ハンドブック」では整理方法などが変更になる場合もあります。

活用して頂くために

製造現場の方々が自らの手で活用できるハンドブックを目指しています。
ご要望があれば、セミナー、講演、勉強会などもお手伝いさせて頂きます。
また、WGへの参画も随時受け付けています。

是非、JNSA西日本支部までご連絡下さい。


JNSA