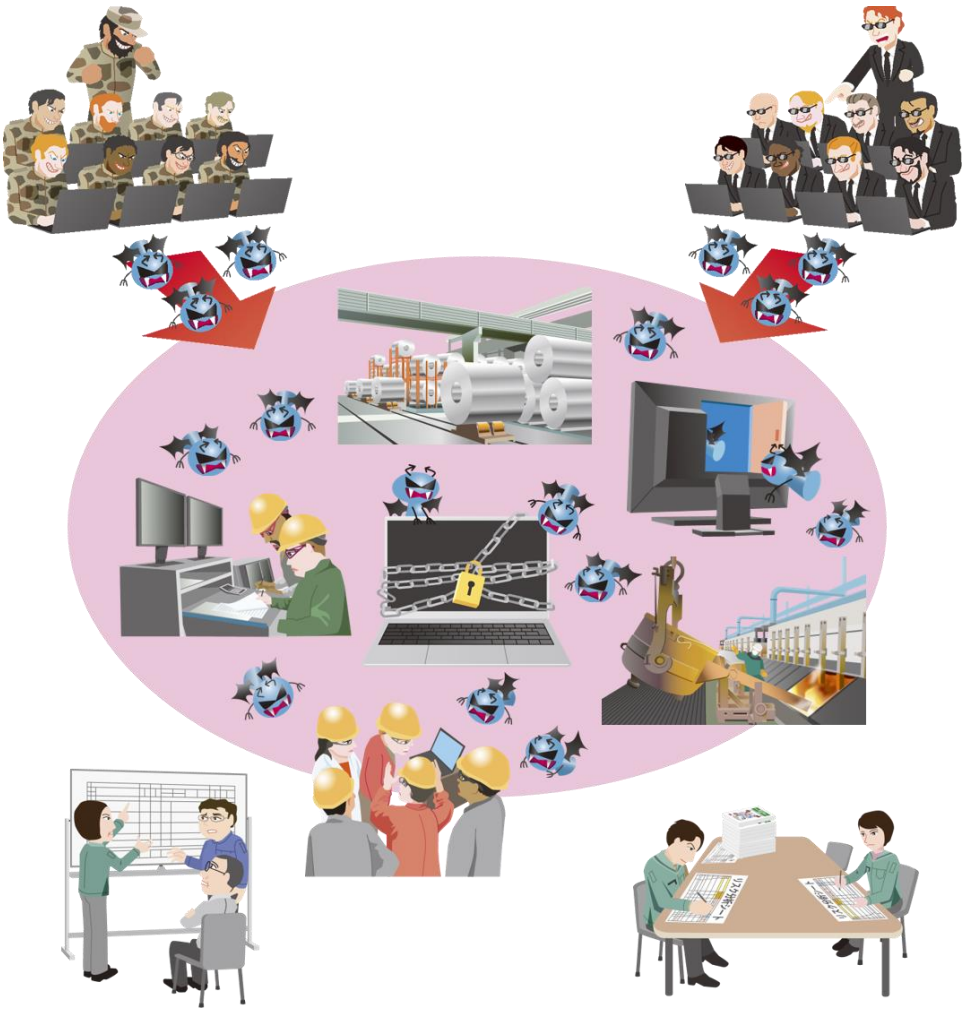
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例5

～2019 年 ランサムウェアによる事業減速～



2025 年 9 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目 次

目 次 2
はじめに 3
1. 2019 年 標的型攻撃＋ランサムウェアによる操業停止 4
1.1. インシデント概要 4
1.2. 被害発生にいたる攻撃の流れ 5
1.2.1. 【攻撃局面 1】対象企業への侵入 6
1.2.2. 【攻撃局面 2】攻撃の足場確立 8
1.2.3. 【攻撃局面 3】本格的な攻撃局面 9
2. リスク分析（事業被害ベース）の素材としてのインシデント情報の整理 10
2.1. 事業被害と攻撃シナリオの検討 10
2.2. 攻撃ツリーの作成 11
2.3. 事業被害ベースのリスク分析の分析要素のまとめ 11
2.4. 対策・緩和策の整理 13
2.5. 攻撃ステップと対策・緩和策の関連付け 14
おわりに 19
参考資料 20

はじめに

「セキュリティ対策を推進する上で、過去の事例に学ぶことは有益です。」

制御システムを保有する事業者にとって、国内外で発生したサイバーインシデント事例の情報をもとに、自社の制御システムに対して同様の脅威が発生した場合のリスクアセスメント（リスクの特定・分析・評価）を実施することは、セキュリティリスク管理の強化につながる。

IPA（情報処理推進機構）は、制御システムにおけるリスクアセスメントの具体的な手順を解説した『制御システムのセキュリティリスク分析ガイド』を公開している。このガイドでは、制御システム保有事業者の事業に重大な被害を与えるサイバー攻撃からの回避に重点を置いた「事業被害ベースのリスク分析手法」を紹介している。自社の制御システムに対して、過去の事例と同様の脅威が発生した場合の事業への影響、脅威の発生可能性、発生した脅威の受容可能性／脅威に対するセキュリティ対策の有効性を分析することは、事業者にとって有益であると考えられる。

「制御システム関連のサイバーインシデント事例」シリーズは、『制御システムのセキュリティリスク分析ガイド』の補足資料として作成した。制御システムのサイバーインシデント事例をもとに、その概要と攻撃の流れ（攻撃ツリー）を紹介している。これらの情報をもとに、事業被害ベースのリスク分析を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することが出来る。

本資料の位置づけ

ランサムウェアによる被害は製造業でも発生している。本書ではその例として、詳細が公開されている、2019 年 3 月起こった標的型攻撃に端を発する世界的なアルミニウム製造企業で発生したランサムウエア攻撃の影響に関する当該企業やセキュリティベンダ等の公開情報（巻末の【参考資料】）をもとに、サイバーインシデントの概要と攻撃の流れを紹介している。
後半では、当該インシデント情報を整理し、前半で取り上げた仮想システムを用いて、攻撃シナリオやツリー・ステップの作成例、対策・緩和策への活用例等、リスクアセスメントの際にどう活用するのかというアプローチを紹介している。
【参考資料】に関しての内容詳細は、リンクから原文を確認いただきたい。本資料では、脚注は上付き番号（例 [1]）、巻末の参考資料はカッコ付き番号（例【1】）で表している。

対象読者

制御システムのリスクアセスメント担当者

1. 2019 年 標的型攻撃＋ランサムウェアによる操業停止

1.1. インシデント概要

2019 年 3 月にノルウェーに本社を置く世界有数のアルミニウム生産企業、Norsk Hydro がランサムウェア『LockerGoga』の被害を受け数カ月の長期間にわたり生産量が低下した。40 か国 160 の拠点で 23,000 台の PC のうち感染が 11,000 台、暗号化されたものが 2,700 台、3,000 台のサーバのうち、1,100 台が感染、500 台が暗号化された[1]。被害を受けた多くはメール、発注や顧客情報管理のコンピュータ等と言われているが、製造用のコンピュータも被害を受けたと推定され、長期間にわたり手作業による製造を強いられた。2019 の Q1 と Q2 合計の損失は、65-77 億円（550-650M ノルウェークローネ）と見積もられている[2]。

Norsk Hydro ではこのインシデントにおいて Transparency（透明性）と Openness（率直さ）をポリシーとし[3]、今後の被害の参考とするため情報公開の姿勢を貫いたことは高く評価[1]されている。

昨今、ランサムウェアによる産業システムへの被害は激増し枚挙に暇がないが、この姿勢から、今回サイバーインシデント事例として取り上げることとした。

サイバー攻撃を受けた Norsk Hydro の状況や取り組みについては同社が作成している4本の YouTube の動画[4]が参考になるが、技術的な情報については 2019 年の CS3sthlm[2]において Norsk Hydro の CISO が行ったキーノートスピーチ[1]にて詳細が語られている。本稿では、その情報に加え各種セキュリティベンダによるマルウェア、ランサムウェアの解析、ノルウェーの Norsk Hydro 本社でのヒアリング等の情報を参考としてまとめている。

今回は、それらの部分的な情報を過去のサイバー攻撃事例の侵入ステップにて補完・推考しながら、最終的なランサムウェア LockerGoga による攻撃までの流れを IEC 62443-2 や NIST SP800-82 Rev.2 等をもとに作成した仮想システム構成図（図 1-1）を用いて説明する。

---

[1] The Norwegian Communication Association's Transparency Award. を受賞

[2] The Stockholm international summit on Cyber Security in SCADA and Industrial Control Systems

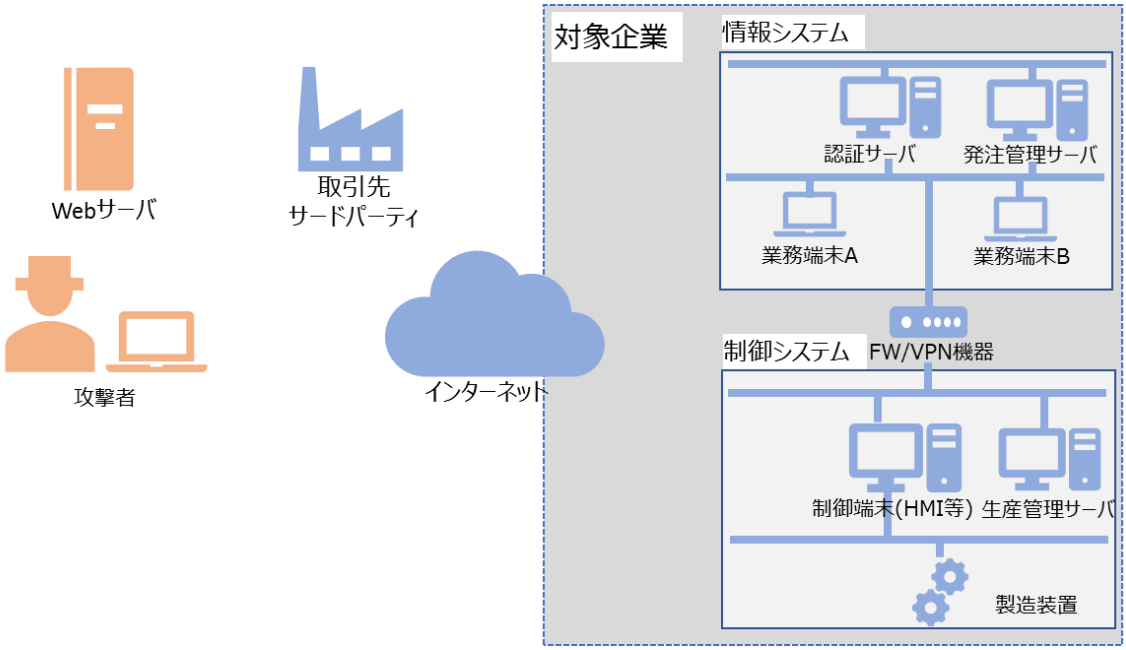


図 1-1 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

1.2. 被害発生にいたる攻撃の流れ

1.2 節では、CS3sthlm で発表された内容にセキュリティベンダの調査結果、現地ヒアリングの結果等を補完することで、サイバー攻撃から被害発生にいたるまでの流れを次の局面に分けて解説する。

① 対象企業（Norsk Hydro）への侵入（1.2.1 項）
② 攻撃の足場確立（1.2.2 項）
③ 本格的な攻撃局面（1.2.3 項）

1.2.1. 【攻撃局面 1】対象企業への侵入

2018/12 以前、攻撃者はまず、対象企業へ侵入するために取引先を攻略。取引先の従業員になりすまし、悪意あるサイトへのリンクを含むメールを対象企業の従業員へ送付した（図 1-2）。[1][7]

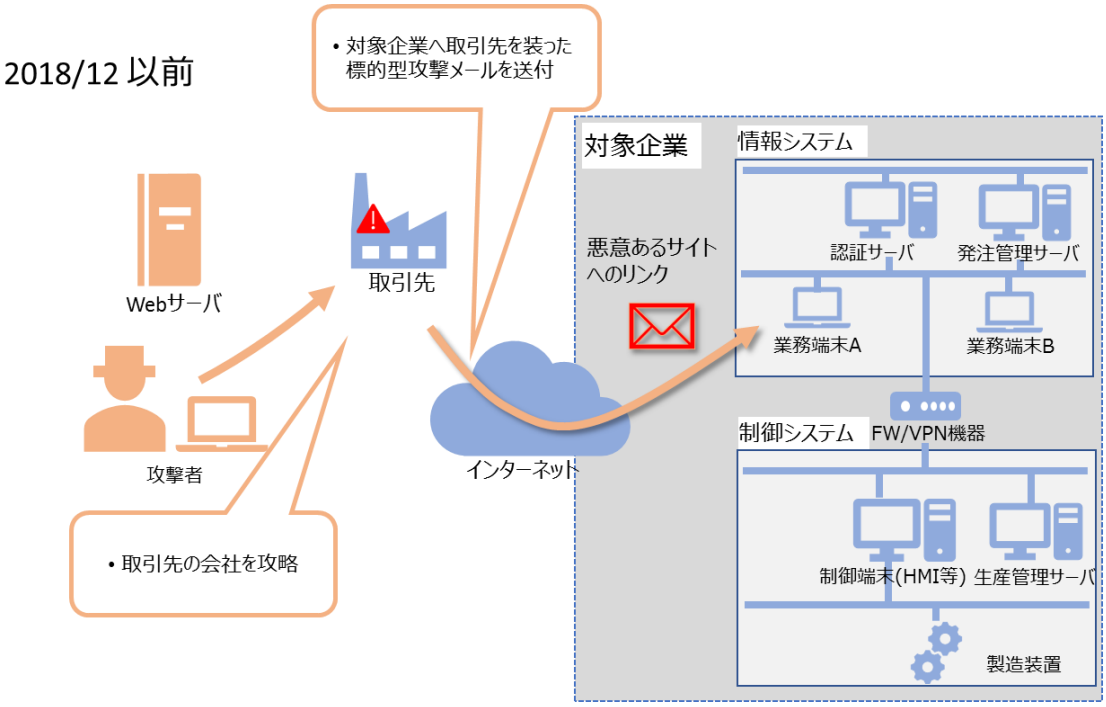


図 1-2 対象企業への侵入（攻撃局面1A）

メールを受信した対象企業の従業員はリンクをクリックし、バックドアを生成するトロイの木馬、GootKit Trojan をダウンロードし感染してしまう[1]。このトロイの木馬は、ファイルのダウンロード機能やパスワード等の機密情報を収集しアップロードする機能等を持つものとして知られている。[5]（図 1-3）

このトロイの木馬が生成したバックドアを通じて対象企業ネットワークの情報を収集する。

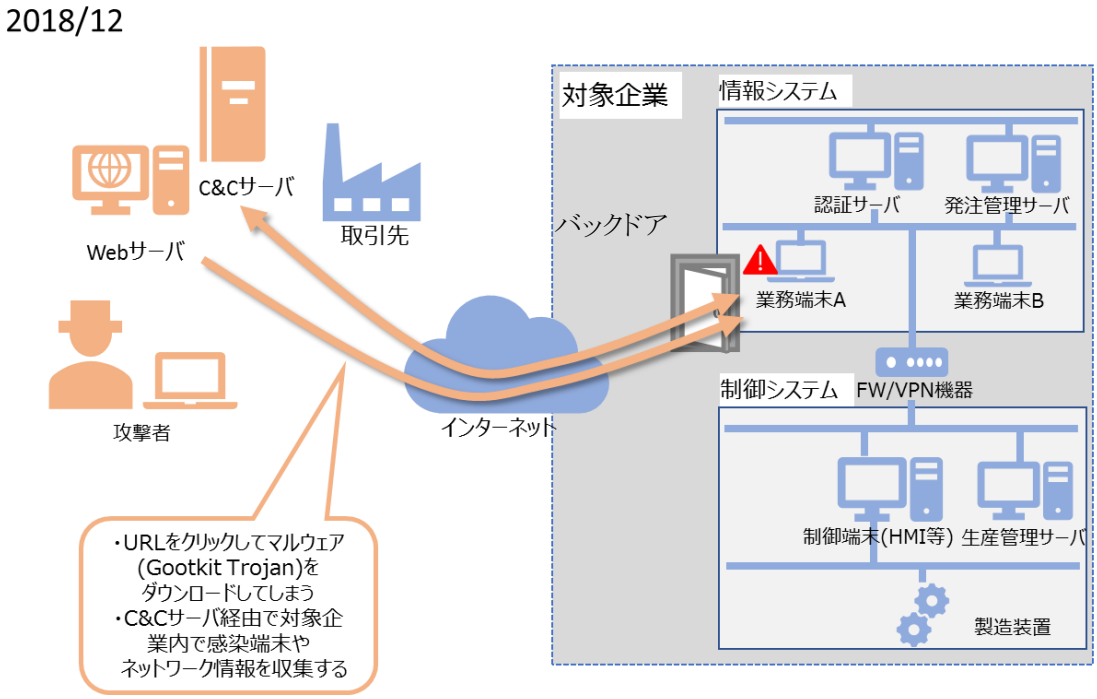


図 1-3 対象企業への侵入（攻撃局面1B）

1.2.2. 【攻撃局面 2】攻撃の足場確立

2019/2 攻撃者は、先に業務端末 A に設置したバックドアを通じて、あらたな攻撃用ツールとして、Cobalt Strike を投入[1]。Cobalt Strike は本来ペネトレーション・テストの支援ツールであるが、悪用される事もあり[6]、本件では高機能の情報収集ツールの役目をはたした。次に攻撃者は、特権の取得や対象企業ネットワークのアカウント情報を取得。認証サーバ(ドメインコントローラ)の管理者権限を用いて攻撃可能範囲を広げる[7]。

このような工程を経て対象企業のネットワークを広範囲に支配下に置くと、最終攻撃用のランサムウェア、LockerGoga[8]を支配下のコンピュータに配布する。(図 1-4)

なお、制御システムは境界 FW によって保護され被害は無かったとの事。

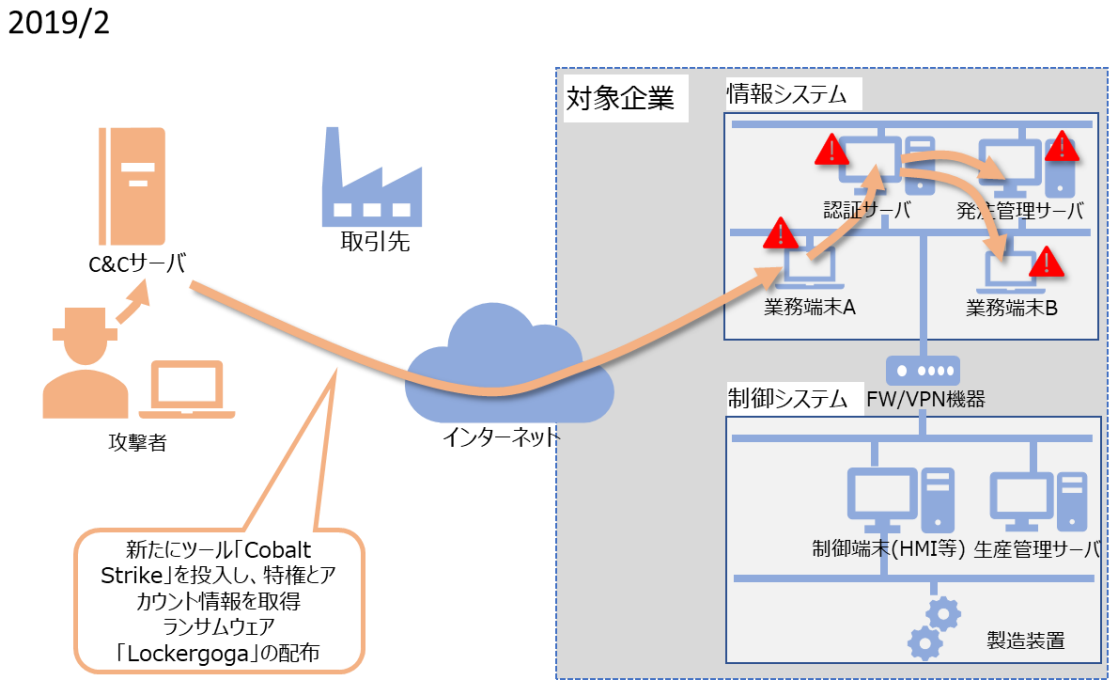


図 1-4 攻撃の足場確立

1.2.3. 【攻撃局面 3】本格的な攻撃局面

2019/3/18-19 複数のコンピュータでほぼ同時期に起動したランサムウェア LockerGoga は、管理者アカウントのパスワードを変更し対象企業の管理者がログオン出来ないように[4]、システムを停止する事もできなくしたうえで、コンピュータ内のファイルを次々と暗号化していく。暗号化が完了すると、すべてのネットワーク接続を遮断し、最後に証拠を残さぬよう自分自身を削除する。また、Windows のブートローダーも暗号化するため、再起動すると OS が立ち上がらなくなる。(図 1-5) [8]

製造事業への影響として、IT システムが使用できなくなったことにより、IT システムから OT システムへの製造指示等ができなくなり、いくつかの工場で操業縮小や一時的な操業停止があった。また、操業を止めることができない工場では、コンティンジェンシープランに基づき、手動により操業を継続した。

なお、攻撃者の意図は不明とのこと。

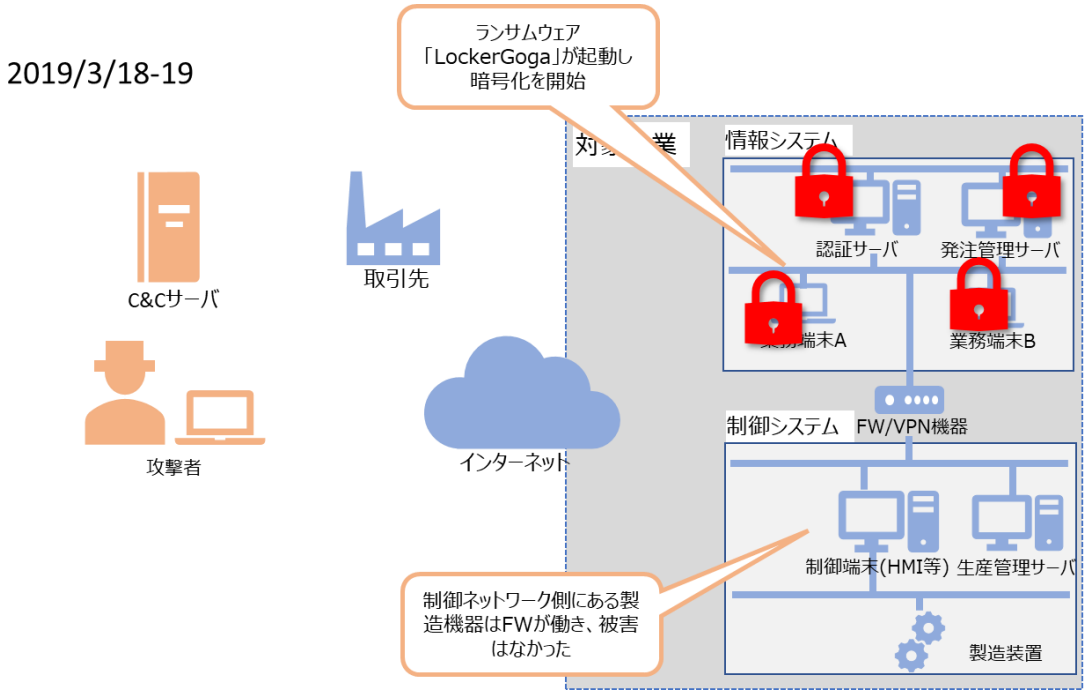


図 1-5 最終的な攻撃局面

[4] LockerGoga の作動には管理者権限が必要

2. リスク分析（事業被害ベース）の素材としてのインシデント情報の整理

2.1. 事業被害と攻撃シナリオの検討

本インシデントを参考に、一般化した形で検討した事業被害の例を表 2-1 に示す。

事業被害 1 は、本インシデントにより発生した事業被害であり、事業被害を引き起す可能性のある攻撃シナリオもあわせて記載する。2.2 節では、この事業被害 1 と攻撃シナリオに至る攻撃ツリーを検討する。

表 2-1 事業被害の例（攻撃拠点、攻撃対象は多数有）

項番	事業被害			
1	製造関連コンピュータの暗号化による工場の操業停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	標的型メールによりマルウェアが組織内ネットワークに侵入。バックドアから内部の管理者アカウント情報を取得され、製造関連コンピュータが暗号化される	認証サーバ	制御端末	ランサムウェアによる暗号化

また、事業被害 1 に至る攻撃ルートの例を表 2-2 に示す。対象企業のシステム構成図、攻撃者、経由に相当する情報は明らかになっていないため、仮説としている。

表 2-2 攻撃ルートの例（斜線アンダーラインは仮説）

誰が	どこから	どうやって	どこで		何をする
攻撃者	侵入口	経由	攻撃拠点	攻撃対象	最終攻撃
悪意のある外部の第三者	*業務端末 A*	*不明*	*認証サーバ*	*制御端末*	ランサムウェアによる暗号化

2.2. 攻撃ツリーの作成

今回のインシデント事例をリスク分析における攻撃ツリー・ステップの枠組みにあてはめ整理した内容が、表 2-3 となる。分析対象の範囲等によっては、切り出し方のパターンは考えられるが、一例として参照いただきたい。

表 2-3 業務端末からの制御システムへの感染・攻撃実行の例

攻撃局面	項番	攻撃シナリオ 攻撃ツリー・ステップ ＜標的型メールによりマルウェアが組織内ネットワークに侵入。バックドアから内部の特権情報を取得され、製造関連コンピュータが暗号化され生産停止＞
【1】	S1	侵入口=業務端末 A 攻撃者が悪意あるリンクを含むメールを送信し悪意あるサイトへ誘導する
【1】	S2	業務端末 A がトロイの木馬に感染し C&C サーバとの通信が確立する。
【1】	S3	攻撃者は、C&C サーバから業務端末 A 経由で対象企業のネットワークやアカウント情報を調査し、次の武器[5]を準備
【2】	S4	収集した情報をもとにマルウェアを投入し、認証サーバ等の特権、アカウント情報を窃取、管理者権限で認証サーバ等からランサムウェアをネットワーク内のコンピュータに配布する
【3】	S5	特定の日時にランサムウェアを起動させコンピュータを暗号化。コンピュータが使えなくなり製造が停止する。

【コラム】Norsk Hydro 社のバックアップ

Norsk Hydro では 3/18-19 にランサムウェアの攻撃を受けたが、4/1 には主要な IT システムの復旧が出来た。これは強固なシステムによるバックアップが残っていたためだったとの事。また一部のオーダー管理では紙ベースにこだわっており、ランサムウェアの影響を受けずに済んだとの事だった。

しかしながらすべてのアプリケーションを完全に戻すには 3 か月の時間を要した。

事業被害ベースのリスク分析の分析要素のまとめ

[5] Norsk Hydro では Cobalt Strike が用いられた。

本インシデントをリスク分析の際の素材として活用するために、1.2 節で紹介した攻撃局面を分析ガイドで説明している事業被害ベースの分析要素毎にまとめた結果が表 2-4 となる。

表 2-4 各種情報をもとにした分析要素のまとめ

分析要素		内容
攻撃用途		
	侵入口	情報システムの業務端末
	攻撃対象	制御端末（製造装置を操作するためのコンピュータ）等
	攻撃拠点	認証サーバ等（管理者権限情報を保有しマルウェアを配布できるサーバ）
	経由	ー
攻撃者		詳細は不明（悪意のある外部の第三者）
事業被害		製造関連コンピュータの暗号化による工場の操業停止
攻撃シナリオ		標的型メールによりマルウェアが組織内ネットワークに侵入。バックドアから内部の特権情報を取得され、製造関連コンピュータがランサムウェアに暗号化され生産停止。
最終攻撃（目的）		ランサムウェアによるシステムの暗号化
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-3 を参照
攻撃手法		標的型攻撃メールの送付 C&C（Command & Control）サーバとの通信確立 情報探索 感染拡大（横断的侵害） リモート接続 特権の取得 ランサムウェアのインストールと実行

リスク分析を進める上では、日々の活動を通じて実際のインシデント事例等の情報収集を行い、最新動向をキャッチアップし、事例毎に表 2-4 のように整理した情報を蓄積していくことが肝要となる。

2.3. 対策・緩和策の整理

対策・緩和策の検討を進める上で、一般的な観点から、ランサムウェアに関しては、CIS[6]から公開された Security Primer – Ransomware[9]、また、標的型攻撃に関しては、IPA から公開された、「高度標的型攻撃」対策に向けたシステム設計ガイド[10]等を参考にして、リスク分析作業に活用するための安全計装システムに対する緩和策を整理した。表 2-5 は、代表的な対策・緩和策をまとめたものとなる。

表 2-5 代表的な対策・緩和策の例

項番	対策・緩和策
D1	システムのバックアップを作成し、リストアの確認を行う[9]
D2	電子メールの添付ファイルを開くことやリンクをクリックすることに注意する[9]
D3	システムが最新のパッチで更新されていることを確認する[10]
D4	インシデントレスポンスプランを策定し、トレーニングを行う[10]
D5	最小特権の原則の順守[9]

「D1. **システムのバックアップを作成し、リストアの確認を行う**」は、ランサムウェアによって暗号化された場合は、あらかじめバックアップしたデータからリストアするしか確実な対応策が無い。ランサムウェアによっては、共有フォルダや接続された外部記憶媒体のバックアップやボリュームシャドウコピー[7]を削除するものもあるため、バックアップデータをオフラインで保管するのが望ましい。また、定期的にバックアップが取得できているかの確認も行う。

「D2. **不明または未確認の送信者からの電子メールおよび添付ファイルを開くことに注意する**」は、人的ミスによるところが大きいが、昨今の標的型メールは、ターゲット組織の関係者を装った内容やアドレスからのものもあるため、既知の人からのメールでもマクロの展開やリンク先のアクセスには十分に注意する必要がある。また、模擬メールによるトレーニングも有効である。

「D3. **システムが最新のパッチで更新されていることを確認する**」は、特に脆弱性を利用したランサムウェア（例えば WannaCry[11]の場合）の一般的な対応策となる。

「D4 **インシデントレスポンスプランを策定し、トレーニングを行う**」は、緊急時にすぐに対応が可能となるようにすべきことをまとめ、組織の体制を構築し、日常から備えておくという意味である。

「D5 **最小特権の原則の順守**」は、ユーザが職務を遂行するために必要な最小限のアクセスレベルを設定するという事である。

---

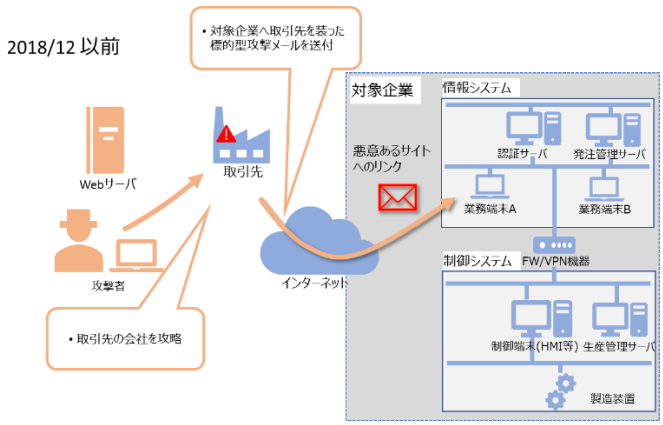
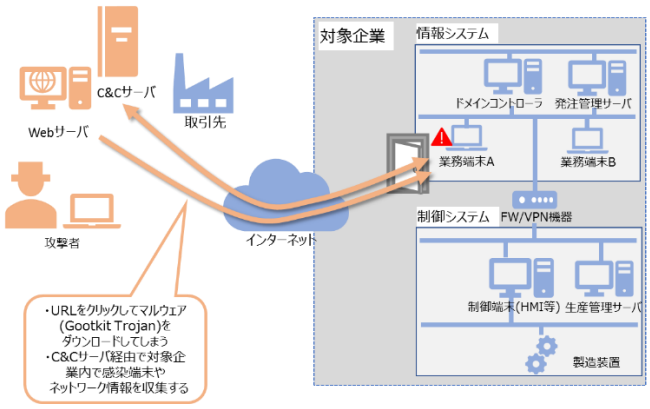
6 Center for Internet Security https://www.cisecurity.org/

7 アプリケーションやシステムを稼働したままバックアップできる Windows の機能

2.4. 攻撃ステップと対策・緩和策の関連付け

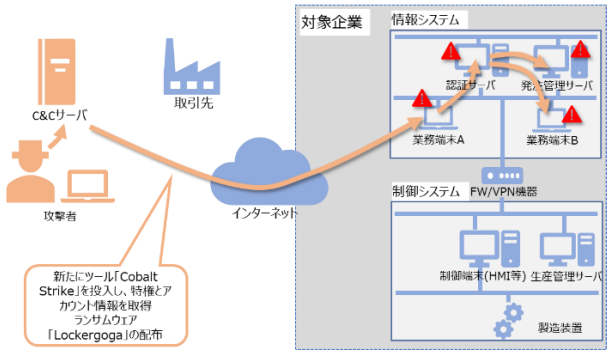
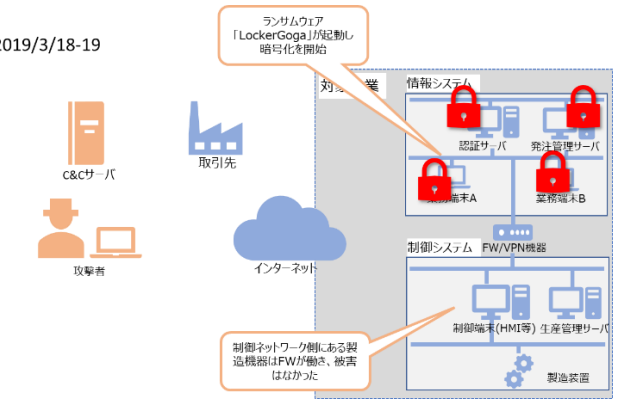
2.3 節までの情報をもとに、各攻撃ステップにおける代表的な対策・緩和策を紐づけた例が表 2-6 となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

表 2-6 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

攻撃局面	攻撃ステップ[8]	対策・緩和策[8]	対象システム・資産
【攻撃局面 1A】  	トロイの木馬に感染 [S2]	•アンチウィルス[9] •振舞い検知 •アンチウィルスのパターンファイル更新	•業務端末
【攻撃局面 1B】  	初期段階の内部調査 [S2]	•ログ収集分析 •パケットキャプチャ •最小特権の原則の順守【D5】 •アカウント管理【D6】	•情報系システム •制御系システム

[8] [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

[9] Gootkit の様に亜種がある場合は検知できない可能性があることを想定する必要はある。

攻撃局面（つづき）	攻撃ステップ	対策・緩和策	対象システム・資産
【攻撃局面 2】 2019/2  	アカウント情報の窃取・ランサムウェアの配布 [S4]	•最小特権の原則の順守【D5】 •アカウント管理【D6】 •エアギャップによる制御系の分離、一方向ゲートウェイ •境界 DMZ の設置	•情報系システム •制御系システム
【攻撃局面 3】 2019/3/18-19  	ランサムウェア起動によりコンピュータを暗号化【S5】	•振舞い検知 •システムのバックアップとリストア【D1】 •インシデントレスポンスプラン【D4】	•情報系システム •制御系システム

【補足説明】

- ランサムウェアに対する対策として、情報系として一般的な対策は、例えば IPA が公開しているランサムウェア特設ページ[12]の中にある、「感染が拡大中のランサムウェアの対策について（2017/6/30）[13]」、Security Primer – Ransomware[9]等に掲載されている、最小特権の原則の順守や定期的なバックアップ等を行う。

- すでに暗号化されてしまったケースへの対応は、一部のランサムウェアに対してではあるが、ID Ransomware[14]、No More Ransom Project[15] 等のランサムウェアデータベースサイトでランサムウェアの特定や暗号化の解除キー（復号キー）を提供している。

- 攻撃ステップ S3 から S4 において、攻撃者がマルウェアやツールを効果的に活用するためには管理者権限が必要となるため（例えば[8]）、ローカルコンピュータの管理者アカウント、OS やアンチウィルスのアップデート管理サーバのアカウントやドメインの管理者等、高い権限を持つアカウント保護に特に注力すべきである。
  具体的な対策として、計算機のアカウントやパスワードの管理を徹底する、パスワードはデフォルトのまま利用しない、単純なパスワードを利用しない、パッチの適用を徹底する。
  これらの基本的な対策に加え、計算機のアカウントの設定に関しては、

  - メール送受信等日常業務を行うためのユーザアカウントには、管理者権限を与えないこと[10][11]。
  - 管理者権限を持つアカウントは、計算機毎や機能毎に管理すること[10]。

  が可能か否かを検討すべきである。（図 2-1）
  また、管理者アカウントによるコンピュータへの不正なログオンの監視も有効である[17]。
  さらに、パスワードそのものではなくハッシュ化[10]されたパスワード等のクレデンシャル情報を窃取し悪用されるケースもあるため、クレデンシャル情報の保護も検討する。[10][18][19][20]

  制御システムの場合は、制御ネットワーク側のアカウントと情報ネットワーク側のアカウントやパスワードが異なるものとなれば（例えば、制御ネットワーク側と情報側のドメインで信頼関係を構築しない）、万が一情報ネットワーク側のドメインの特権アカウントが窃取されてしまっても、制御ネットワークが情報ネットワークと同時に侵入されてしまうというリスクは低減できる[16]。

[10] 元のデータを一定の計算手順に従って規則性のない固定長の値に変換すること

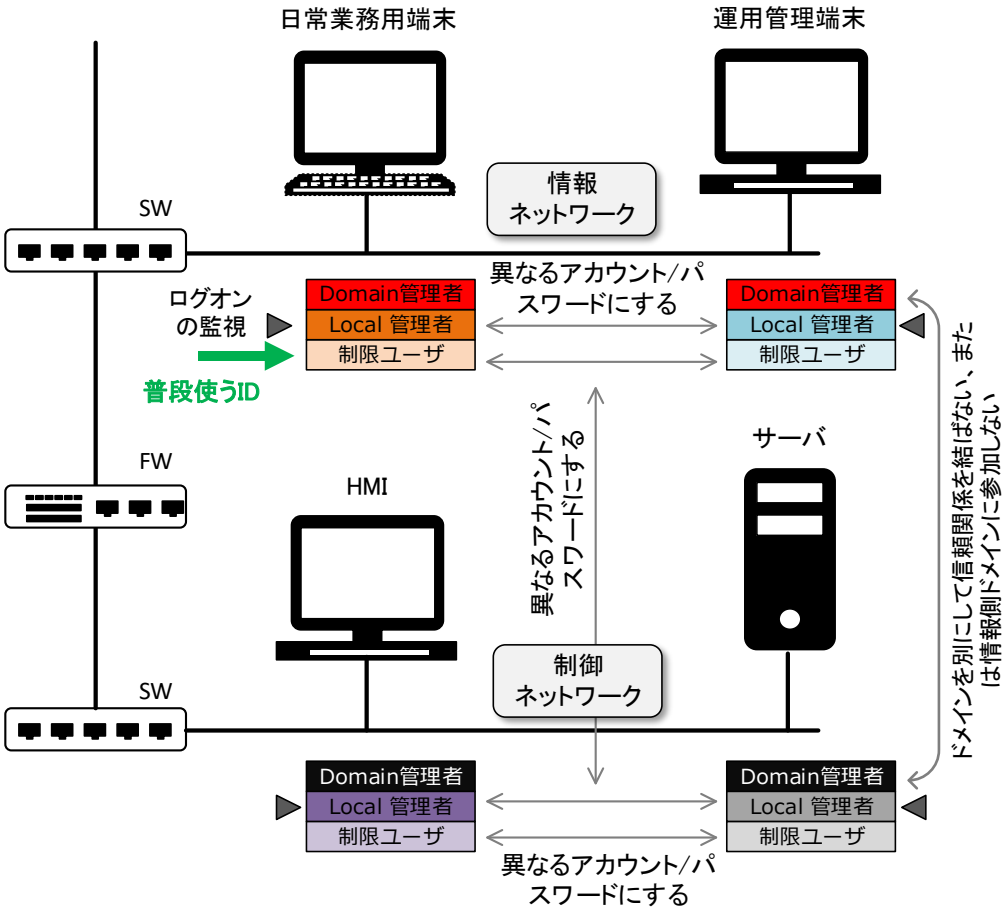


図 2-1 アカウント/パスワードの管理

- 攻撃ステップ S4 において、Cobalt Strike[11]のようにディスク上にファイルとして保存されない高度なツールの場合、ファイルのシグネチャ情報のみを利用する方式のアンチウィルスでは検知できない。検知の可能性を上げるには、一部のヒューリスティック（ふるまい検知）方式のものや、レジストリやシステムフォルダの監視等も含む総合的な監視/検知系のソフトウェア等が必要となる[10]。

  また、PowerShell 等のマイクロソフトが提供するシステム管理用ツールも頻繁に攻撃に利用されている。これらは本来管理用ツールなので、管理のための実行と悪意による実行を区別するのは困難である。PowerShell 等の管理ツールが必要な場合は、ログ機能を持つバージョン 5.0 以上の PowerShell をインストールして動作ログを取り監視する[21]。また、製造現場のコンピュータの様にこれらのツールによる集中管理が不要であれば、PowerShell のセキュリティポリシーにより実行を制限したり、禁止したりする[9]。

- 攻撃ステップ S5 において、ランサムウェアによるファイルの暗号化プロセスは高度化され検知が困難なケースが多い。例えば LockerGoga では、有効なデジタル署名が付与されていたり多数の暗号化スレッドが起動したりする等[8]、検知を回避するためと推定されるような工夫がなされている。

  また、ランサムウェアによっては、暗号化はオンラインのバックアップデータにまで及ぶ場合がある。

  このような実態を踏まえたうえで最も確実な対策と考えられるのは、オフラインでバックアップを保管すること、暗号化されたシステムをすみやかにバックアップからリストアできるようすること、暗号化されて使えなくなった製造用コンピュータを使わずに手動操作ができるような手順について等、日常からトレーニングを行うことである。[9]。

[11] 詳しくは Cobalt Strike Beacon

おわりに

本資料では、制御システムにおけるインシデント事例を紹介すると共に、セキュリティリスクアセスメントへの活用方法について一つのアプローチを紹介した。

事業被害ベースのリスク分析においては、自社の制御システムにとって回避すべき事業被害を明確化し、被害に至る攻撃シナリオを漏れなく洗い出すことが重要である。攻撃シナリオは、過去に発生した制御システムのインシデント事例を含む各種の公開情報を参考にしつつ、自社の制御システムに生じ得る脅威とその影響を検討するが、具体的な攻撃手順を想定することで、セキュリティ対策を効率的に進めることが可能となる。

本資料が各社の制御システムのセキュリティ向上に活用されることを期待する。

参考資料

[1] CS3sthlm:
https://cs3sthlm.se/
詳細はリンク切れ。発表があった事だけが記載されている
https://cs3sthlm.se/（初版発行時）
第 2 版発行時詳細はリンク切れ。発表があった事だけが記載されている

[2] Norsk Hydro: Cyber-attack on Hydro（2019/11/14　Updated: May 15, 2024）
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

[3] Norsk Hydro: Hydro awarded for cyber-attack transparency（2019/9/21　初版発行時）
https://www.hydro.com/en-NO/media/news/2019/hydro-awarded-for-cyber-attack-transparency/

[4] Norsk Hydro: YouTube
Cyber attack on Hydro Magnor
https://www.youtube.com/watch?v=S-ZlVuM0we0
How one ransomware attack cost £45m to fix - BBC News
https://www.youtube.com/watch?v=7yHsiTmUnPk
Why Hydro chose to be transparent during cyber-attack
https://www.youtube.com/watch?v=C6MDz-AgQuE
The cyber attack rescue operation in Hydro Toulouse
https://www.youtube.com/watch?v=o6eEN0mUakM

[5] トレンドマイクロ: Trojan GootKit（2018/12/19）
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/malware/trojanspy.win32.gootkit.aa

[6] JPCERT/CC: Cobalt Strike Beacon を検知する Volatility Plugin（2018-07-31）
https://blogs.jpcert.or.jp/ja/2018/07/cobaltstrike.html
Cobalt Strike:
https://www.cobaltstrike.com/

[7] Microsoft: Hackers hit Norsk Hydro with ransomware. The company responded with transparency（2019/12/16）

https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[8] 三井物産セキュアディレクション: LockerGoga の内部構造を紐解く(2019/8/27)
https://www.mbsd.jp/blog/20190827.html
トレンドマイクロ: 暗号化型ランサムウェア「LockerGoga」について解説(2019/4/8)
https://blog.trendmicro.co.jp/archives/20840

[9] CIS: Security Primer – LockerGoga
https://www.cisecurity.org/insights/white-papers/security-primer-lockergoga

[10] IPA:「高度標的型攻撃」対策 に向けたシステム設計ガイド(2014/9)
https://www.ipa.go.jp/files/000046236.pdf

[11] CIS: Cyber Alert: WannaCry Ransomware (2017/5/15)
https://www.cisecurity.org/ms-isac/cyber-alert-wannacry-ransomware/

[12] IPA: ランサムウェア特設ページ(2018/2/16)
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

[13] IPA: 感染が拡大中のランサムウェアの対策について(2017/6/30)
https://warp.da.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/security/ciadr/vul/20170628-ransomware.html

[14] ID Ransomware
https://id-ransomware.malwarehunterteam.com/

[15] No More Ransom Project
https://www.nomoreransom.org/ja/index.html

[16] CISA: Alert (TA18-276A) Using Rigorous Credential Control to Mitigate Trusted Network Exploitation(2018/10/3)
https://www.us-cert.gov/ncas/alerts/TA18-276A

[17] JPCERT: 攻撃者の行動を追跡せよ(CODE BLUE 2017)
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

[18] JPCERT/CC：Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard（2016-09-07）
https://blogs.jpcert.or.jp/ja/2016/09/lsa_protect.html
[19] JPCERT/CC：ログを活用した Active Directory に対する攻撃の検知と対策（1.2 版）（2018/7/28）
https://www.jpcert.or.jp/research/AD_report_20170314.pdf

[20] FFRI：windows10_セキュリティ評価支援報告 Phase2（2017/3/23）
https://www.ffri.jp/assets/files/research/research_papers/windows10_security2_ja.pdf

[21] IPA：標的型攻撃の実際と初動調査の紹介（2018/10/18）（初版発行時）
https://www.ipa.go.jp/files/000069700.pdf

更 新 履 歴

2020 年 3 月 16 日	初版	ー
2025 年 9 月 25 日	第 2 版	現地のヒアリングをもとに加筆修正

制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 5

～2019 年 ランサムウェアによる操業停止～

[発　　行]　2025 年 9 月 25 日 第 2 版

[著作・制作]　独立行政法人情報処理推進機構 セキュリティセンター

編集責任　辻 宏郷

執筆者　福原 聡

協力者　桑名 利幸　木下 弦　小助川 重仁　木下 仁　高見 譲