JPCERT CC®

ICSセキュリティポリシーの現場への浸透および具体化に関する支援検討

参天製薬株式会社
Digital&IT本部 Global Cybersecurity Manager 正木 文統

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ 堀 充孝

アジェンダ

- 本講演の目的
- 取り組みの背景・課題
- 文書の概要
- 対談：今回の活動について
- おわりに

本講演の目的

- 自組織のICSセキュリティポリシー（以下、「ポリシー」という。）を策定後、実効性をもって対策を浸透させるには非常に時間がかかる
  - ICSの現状に合わせた対策を検討
  - 対策の実施に向けた製造現場の関係者との調整

- そうした状況の中、製造現場の関係者に向けて次の点をまとめた
  - ICSにおける実際のセキュリティリスクとは何なのか
  - 対処すべき方法としてどのような方法があるのか

- 現場への浸透をより効率的に実施するための手引きを作成するに至った背景および文書の概要などについて紹介

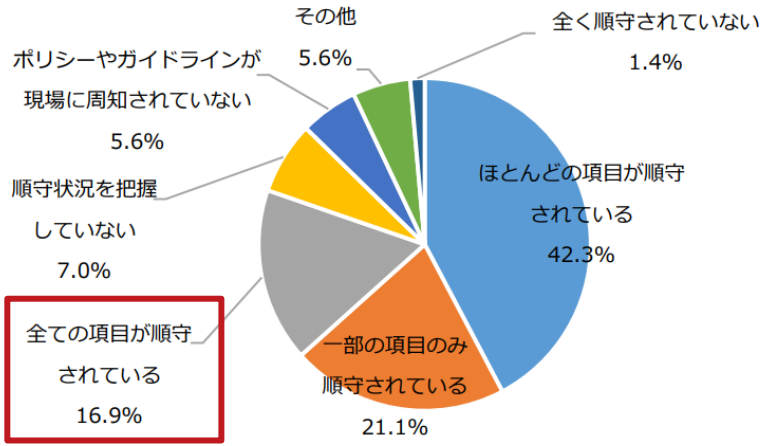
取り組みの背景・課題

JPCERT/CCから見える背景・課題（1）

- ポリシーを作成している組織は多く見られる
  - 一方、複数のICSユーザー組織から「製造現場への浸透には苦慮している」と伺う
- 制御システムセキュリティカンファレンス2023のアンケート結果
  - 作成されたポリシーの「全ての項目が順守されている」とする回答者は2割以下
  - アンケート結果からも、各組織が対応に苦慮している様子が伺える

制御システムセキュリティカンファレンス2023のアンケート設問

貴組織での制御システムの運用において、貴組織の制御システムセキュリティポリシーやガイドラインで規定されている項目が順守されていますか？



JPCERT/CCから見える背景・課題（2）

- ICSセキュリティ関連の標準やガイドライン（IEC62443シリーズやNIST SP800-82、NIST CSFなど）は概念的な内容が多い
  - 製造現場の実態を踏まえ、 ICSユーザー自身でルールや手順の落とし込みが必要

- ポリシーに沿ったルールや手順の作成にはIT技術に詳しくない工場関係者との連携・協力が不可欠

- 製造現場にルールを落とし込む上でIT/OTセキュリティ担当者および工場関係者がどのようなアクションを取るべきかを記した文書は、これまで示されていない

参天製薬株式会社から見える課題（1）

■ これまでの制御システムセキュリティカンファレンスでの講演

年	講演タイトル	主な内容
2021	制御セキュリティポリシー導入における課題と解決のヒント	✓ セキュリティポリシー策定の背景 ✓ ポリシー策定のステップ ✓ 各ステップにおける課題と解決策
2023	どうする？これからの制御セキュリティ	✓ ポリシーを現場に実装するにあたっての課題と対応策 ✓ 更なるセキュリティ向上に向けてのチャレンジ

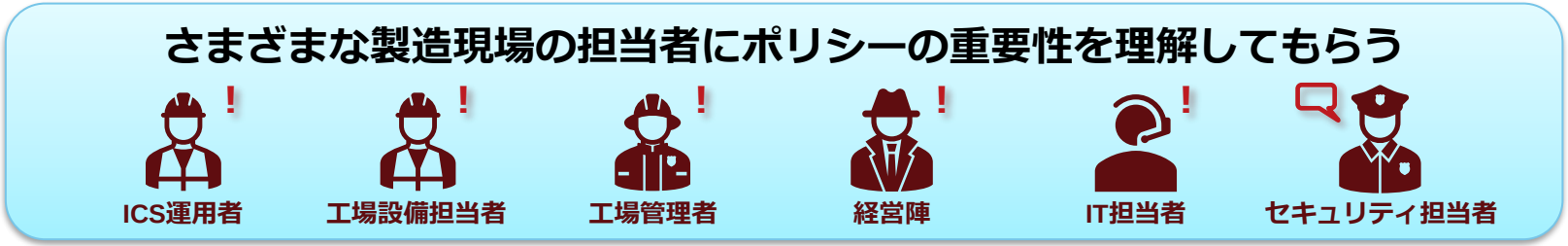
参天製薬株式会社から見える課題（2）

- これまでの講演で伝えてきたこと
  - ICSセキュリティ対策を現場で実施するためには
    - さまざまな場面で障壁があり、対策の理由やどこまで実施すれば良いのかを現場の皆さんに理解してもらいながら、自分事として捉えて実施してもらう（本当の意味での浸透をしていく）には非常に時間がかかる

- ポリシーを現場に浸透し、具体化する上での課題
  - ポリシー自体は概念的、抽象的な内容が多く、具体化に時間がかかる
  - 会社独自のプロセスや環境が原因で、リスクの把握とそれに合わせた対策検討が難しい
  - 現場で関係者が共通解を持つには時間も労力もかかる

課題のまとめ

- ポリシーの製造現場への浸透には労力がかかる



- 工場のセキュリティ担当者は兼務が多く、ICSセキュリティ対策にあまり工数を割けない
  - 情報システム部門との兼務、設備部門（計装部門）との兼務 など

解決に向けたICSユーザー組織への支援検討

■ 課題解決に向けた支援の方向性

ICS運用者がポリシーを順守する際の必要事項をまとめた文書を作る

より製造現場の実態に即した具体的な内容にする

各組織で必要な要素※を取捨選択できるようにし、セキュリティ担当者の工数を削減する

※管理対象、実施すべきルールなど

それぞれの知見を持ち寄る

製薬業界版を作成

一般製造業向けに調整

文書の概要

文書の方針

- 想定読者
  - ICSユーザー組織における工場のセキュリティ担当者
  - ICSセキュリティポリシーが作成されている

- 目的：ポリシーを製造現場に浸透させるため、次の3つを支援する

さまざまな製造現場の担当者へのICSセキュリティに関する理解促進

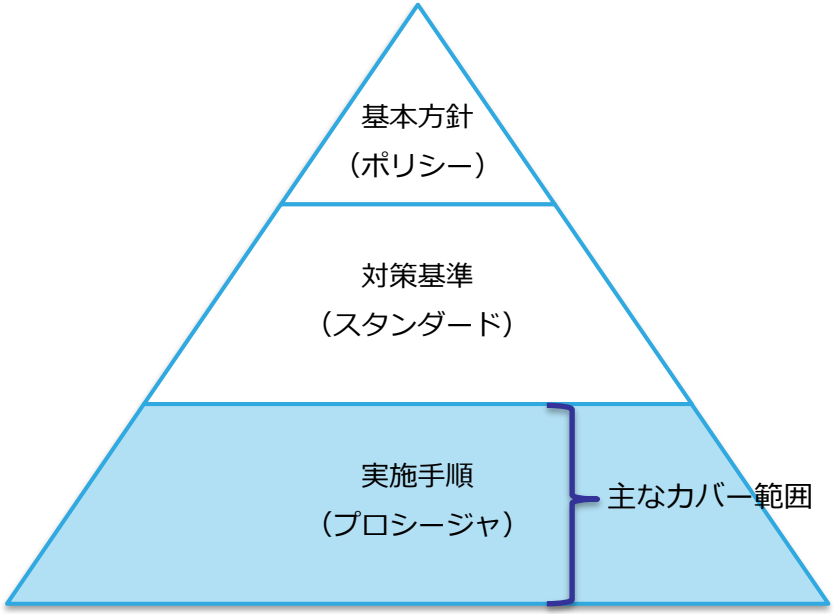
ICS運用者がポリシーを順守するために必要なルールの作成

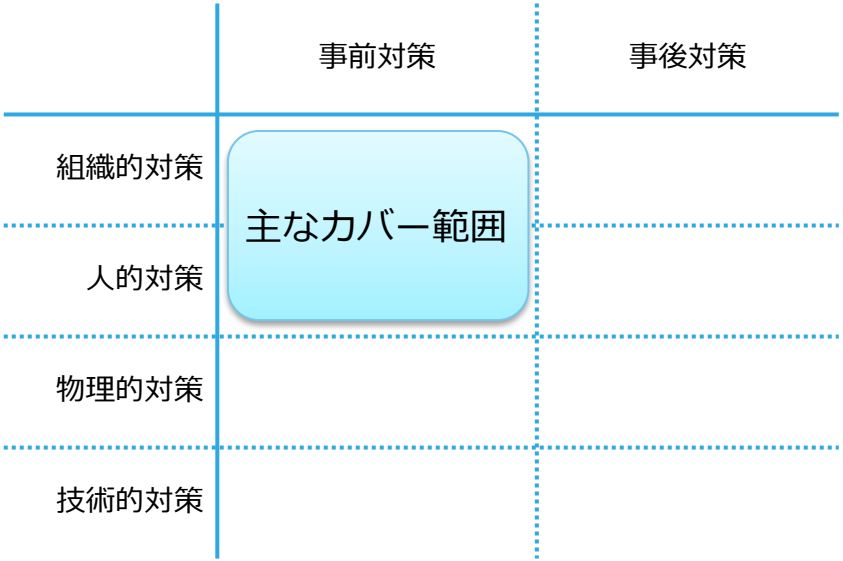
ICS運用者がポリシーを順守するために他の工場関係者が取るべきアクションの整理

文書のスコープ

①ポリシーの具体化を支援する
⇒ プロシージャ中心

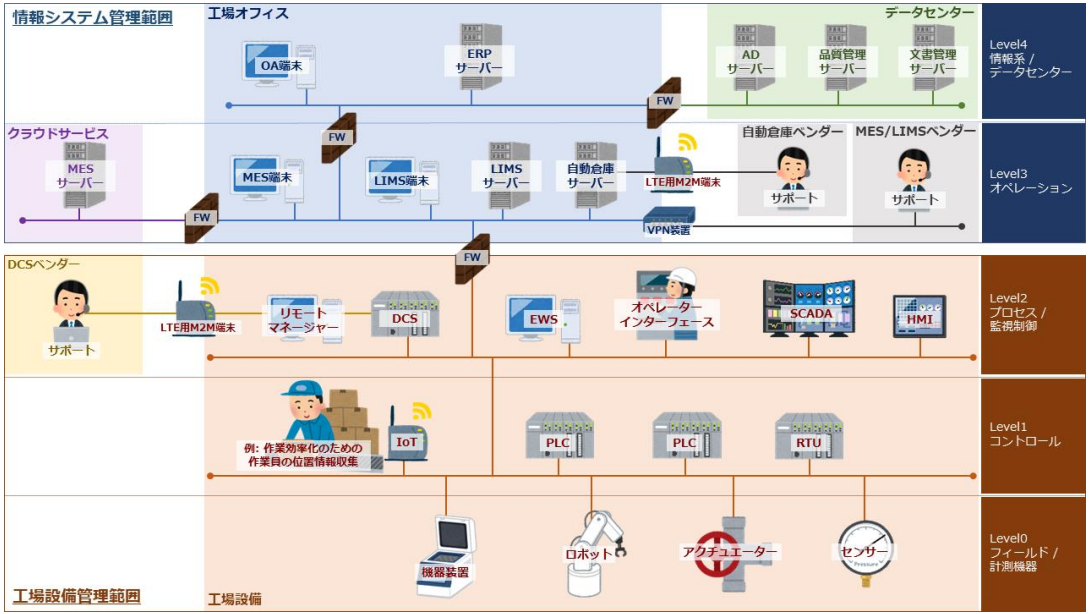
②日々のICSの運用の中に組み込む
⇒ 組織的対策、人的対策中心





想定するシステム

- Purdueモデルをベースに、参天製薬の現状やJPCERT/CCが各組織と実施した意見交換などを踏まえたチューニングを実施
  - 制御情報系のサーバーの一部がクラウド化されている
  - 自動倉庫、MES、LIMS、DCSへのリモートメンテナンスが可能になっている など



文書の構成

■ 次の3つの文書を作成する

ICSセキュリティポリシーの
現場への浸透および具体化の手引き

登場人物ごとのアクションリスト
（サンプル）

ICSセキュリティ意識向上テスト
（サンプル）

ポリシーの現場への浸透および具体化の手引き

■ ICS運用者が直接関わる
7つの管理項目が対象

外部記憶媒体


持ち込みPC

アカウント


アプリケーション


メール対応


無線LAN


クラウドサービス

■ 各管理項目について、
次の流れに沿って説明

- 主な用途および使用例
- 使用の際に想定されるリスク
- ICS運用者が順守すべきルール
- その他関係者が順守すべきルール
- 順守すべきルールに基づく利用フロー
- 例外ケースへの対応
- 想定される被害シナリオと過去事例
- 各管理項目に関する参考情報

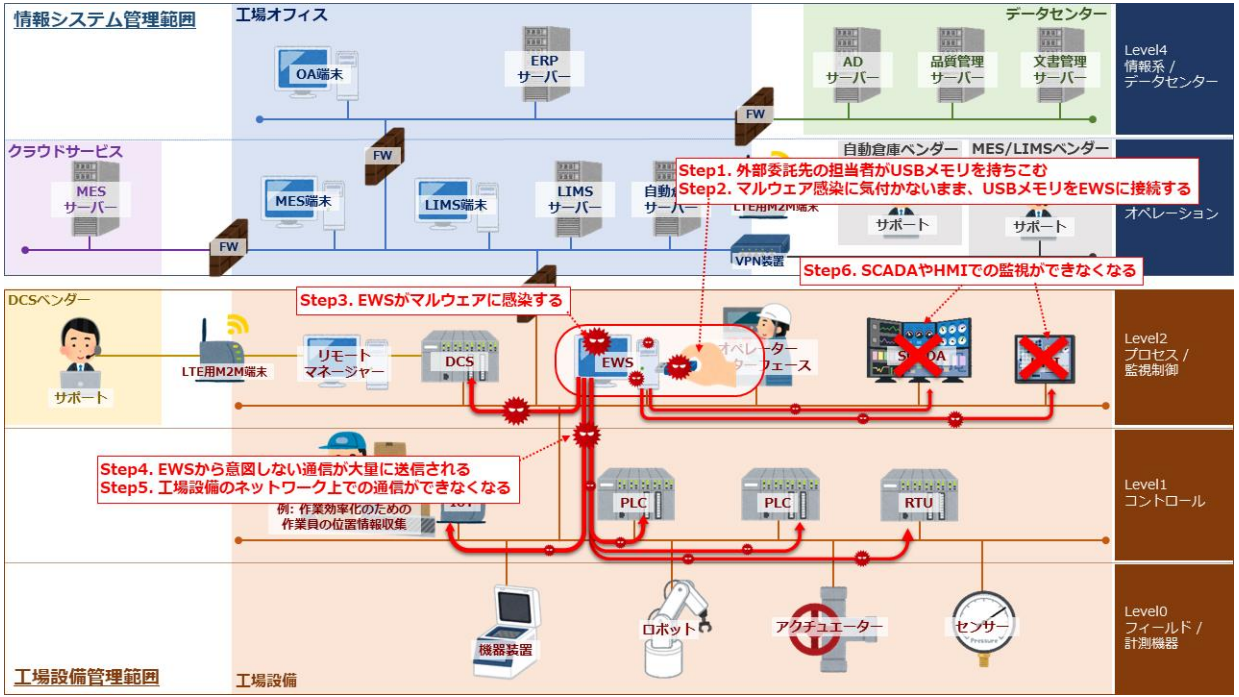
各管理項目・ルールについては、各組織の事情にあわせて取捨選択する

⇒ すべてのルールを実施することを求めるものではない

参考：外部記憶媒体の管理不備による被害シナリオの例

■ 想定されるシステムに対する被害シナリオの例を各管理項目で図示

例：外部記憶媒体の管理不備によって発生する可能性がある被害シナリオ



※今後内容は修正される可能性があります

登場人物毎のアクションリスト（サンプル）

- ICS運用者がルールを順守する際の運用フローの構築の参考として
  - 誰（どの役割の人）が何をするのかを各管理項目ごとに整理
  - そのアクションを実施するかどうかの採否をステータスにて管理

No.	カテゴリ	担当者	サイクル	必須/推奨	アクション	ステータス	備考
1	外部記憶媒体の管理	ICS運用者	日々の運用	必須	媒体管理のガイドラインに従った運用実施		
2	外部記憶媒体の管理	ICS運用者	定期的な運用/点検	必須	媒体管理のガイドライン確認		
3	外部記憶媒体の管理	工場設備担当者	日々の運用	必須	媒体の新規登録・管理		
4	外部記憶媒体の管理	工場設備担当者	日々の運用	必須	媒体管理台帳による媒体の管理		
5	外部記憶媒体の管理	工場設備担当者	日々の運用	必須	未登録媒体利用検知時の対処サポート		
6	外部記憶媒体の管理	工場設備担当者	日々の運用	推奨	不正な媒体利用の検知と対処のサポート		
7	外部記憶媒体の管理	工場設備担当者	定期的な運用/点検	必須	媒体管理の運用状況確認		
8	外部記憶媒体の管理	工場設備担当者	定期的な運用/点検	推奨	媒体棚卸の実施		
9	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体管理台帳への登録		
10	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体貸出申請の受付		
11	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体返却状況の確認		
12	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体の初期化状況の確認		
13	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体管理ルールの周知徹底		
14	外部記憶媒体の管理	工場管理者	日々の運用	必須	所有者不明媒体の設備担当者への報告		
15	外部記憶媒体の管理	工場管理者	日々の運用	必須	ベンダーへの持込み禁止徹底		
16	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体管理に関するトラブルの対処		
17	外部記憶媒体の管理	工場管理者	日々の運用	必須	媒体管理に関するトラブルの報告		
18	外部記憶媒体の管理	工場管理者	日々の運用	推奨	媒体管理ツールへの登録		
19	外部記憶媒体の管理	経営陣	日々の運用	必須	媒体管理実施状況の確認		
20	外部記憶媒体の管理	経営陣	日々の運用	必須	媒体管理に関するインシデント報告受付		
21	外部記憶媒体の管理	経営陣	定期的な運用/点検	必須	媒体管理手順の遵守状況の確認指示		
22	外部記憶媒体の管理	経営陣	定期的な運用/点検	推奨	技術的対策の実施に向けた予算の認可		
23	外部記憶媒体の管理	IT担当者	日々の運用	必須	媒体の新規登録・管理		
24	外部記憶媒体の管理	IT担当者	日々の運用	必須	未登録媒体の利用検知と報告		
25	外部記憶媒体の管理	IT担当者	日々の運用	推奨	不正な媒体利用の検知と対処のサポート		
26	外部記憶媒体の管理	IT担当者	日々の運用	推奨	媒体管理ツールの運用		

※今後内容は修正される可能性があります

意識向上テスト（サンプル）

- e-Learningへの活用を想定してリスト形式のデータで提供予定
  - 問題数は約100問、各組織で問題を取捨選択することを想定
  - 一部、参照する文書を各組織で修正することを前提とした内容の解説がある

No.	カテゴリ	問題	選択肢	正答	解説
1	全般	工場ネットワークは他の情報系ネットワークと隔離されており、インターネットにも接続しないため、セキュリティ対策は必要ない。	はい/いいえ	いいえ	USBメモリなどの外部記憶媒体や持ち込みPC経由でマルウェアに感染するセキュリティインシデントはこれまでも発生しています。インターネットに接続していない、他のネットワークと接続していないICSでも、これらを介して間接的に他のネットワークと接続されるため、注意が必要です。
2	全般	ICSのセキュリティ対策を検討する際、物理的なセキュリティ対策に関しては考慮しなくてもよい。	はい/いいえ	いいえ	セキュリティ対策を施すことによってICS運用に支障が出る場合もありますので、物理的なセキュリティ対策もあわせて検討することが肝要です。 例えば、制御室内にある監視・制御用の操作端末は即時の対応を求められる場合があり、ログイン（ID・パスワードを入力して認証）作業が手間になってしまう可能性があります。そのような場合は、制御室に入れる従業員をIDカード認証によって制限し、操作端末を触れる従業員を制限するといった代替策を検討することになります。
3	全般	古いICS関連機器に脆弱性が見つかったとしても、修正によって保守対象外になってしまうとベンダーから言われてしまっているため、対処できない。	はい/いいえ	いいえ	脆弱性を持つ機器に対し、アップデートの実施やパッチ適用などの根本的な対策ができない場合であっても、リスク軽減策の実施も考えられるため、ベンダーやセキュリティ担当者と一緒に対策を検討してください。 リスク軽減策の例としては、その機器へのネットワークアクセスを遮断する、脆弱性の影響を受ける機能を使用していない場合は無効にするなどが考えられます。
4	全般	情報セキュリティの3要素、「機密性」、「完全性」、「可用性」の3つの要素の内、ICSセキュリティにおいて最も重要視すべき要素はどれか。	機密性、完全性、可用性	可用性	工場で最も重視されるべきことは工場設備を止めないことです。人命、環境、設備、生産性への影響を考えた場合、可用性が最も重要視されます。また、不正なデータが処理されることによって、ICSが意図しない動作をする可能性があることから、データの完全性（データが改ざんされていないことを担保すること）も重要視されます。
5	全般	システムの操作に慣れているので、システムに変更があっても、手順書などの確認はしなくてもよい。	はい/いいえ	いいえ	システムの変更によって、操作が変わることがあるので、手順を確認せずに作業をするのが危険なため。
6	全般	外部からの訪問者が従業員と同行せずに工場内を歩いているのを発見したが、気にせず自分の作業に戻った。	良い/悪い	いいえ	スパイ行為を目的とした敵対者が外部委託事業者として組織に潜り込んだ事例や、外部委託事業者の操作ミスによってマルウェアが工場内に拡散した事例もあります。そのため、定められた手順に沿って対応が行われているかどうか、不審な挙動を行っていないかなどを確認する面から、外部からの訪問者に必ず付き添うようにしてください。 外部からの訪問者が単独で作業をしていることを発見した従業員は、そのエリアの管理責任者に報告してください。

※今後内容は修正される可能性があります

対談：今回の活動について

1. 文書作成の中で注力した点
2. 文書の活用のポイント
3. 文書を作成していく中で新たに見つかった課題

1. 文書作成の中で注力した点

- どうすれば使いやすい文書になるかの検討

- 文書の構成や文書の内容について

作成フェーズ

ICSセキュリティポリシーの
現場への浸透および具体化の手引き

登場人物ごとのアクションリスト
（サンプル）

ICSセキュリティ意識向上テスト
（サンプル）

2. 文書の活用のポイント

■各文書の活用方法

■実施すべきルールの取捨選択について

活用フェーズ

ICSセキュリティポリシーの
現場への浸透および具体化の手引き

登場人物ごとのアクションリスト
（サンプル）

ICSセキュリティ意識向上テスト
（サンプル）

3. 今後の展開について

- 本活動の今後
- 参天製薬の新たな課題について
- 本文書ではカバーできていない部分について

おわりに

まとめ

- 「自組織でICSセキュリティポリシーを策定したものの、実効性が乏しいという課題がある」という方々に向けた支援活動を実施

- 実用性のある文書を目指し、JPCERT/CC＆参天製薬株式会社による共同執筆
  - レビューには製薬組織のセキュリティ担当者に参加していただき、より実務的に使えるようにした

- ICSユーザー組織に広く利用してもらうため、最終的に一般製造業向けの文書をJPCERT/CCにて公表予定

今後の予定について

- 今年度中に一般製造業向けの文書をJPCERT/CCにて公表予定

- 次年度は付録の追加や英語版の作成などを検討する予定

公表まで今しばらくお待ちください

Thank you!