攻撃者グループへの効果的な対策

第１位［特権アカウント管理］
　PowerShellを実行できるユーザーは、グループポリシー等で必要最低限の**管理者のみに制限**する。
第２位［特権アカウント管理］
　SYSTEMやrootを含む**特権アカウント**の作成・修正・使用は**必要最低限**とする。
第３位［ネットワーク侵入防止］
　インディケータを活用しIDS/IPS等によりネットワークレベルの不正を検知・防御する。
第４位［ネットワーク侵入防止］
　メール添付ファイルをスキャンし、悪意のあるファイルを削除する。
第５位［ウイルス対策］
　アンチウイルスソフトのシグネチャ等を最新化し**マルウェアの実行を制限**する。
第６位［ユーザー教育］
　不用意に**メール内のリンクや添付ファイルを開いたりマクロを有効化しない**ようシステム利用者へ周知する。
第７位［ユーザー教育］
　複数のシステムを利用する際に**同じパスワードを使いまわさない**ようシステム利用者へ周知する。
第８位［実行防止］
　ホワイトリスト等で使用可能なコマンドを制限するなど**実行できる処理を制限**する。
第９位［実行防止］
　リモートアクセスに使用できる未承認のソフトウェアのインストールと使用を防止する。
第10位［パスワードポリシー］
　特権アカウントのパスワードは、**複雑**かつ同じネットワーク上にある全てのシステムを通して**一意**のものとする。

大会前に実施しておくと効果的な確認事項

内閣官房
内閣サイバーセキュリティセンター
NISC

大会前の最後の確認１．攻撃経路への対策	
１．インターネットに公開しているWebサービス等の稼働状況確認	インターネットにはWebサービスやメールサービス等、**業務に必要なサービスのみ提供されていることを確認**する。
	アクセス元IPアドレスや証明書等で**アクセス制限を実施しているサービスは、制限範囲が適切か確認**する。
２．攻撃に多く悪用されやすい脆弱性への対策	Windowsシステム（端末、サーバ）に**必要な最新のセキュリティ更新プログラムが適用されていることを確認**する。 ※定期的に確認されている場合は、改めて追加で実施することは不要。
大会前の最後の確認２．アカウントへの対策	
３．業務利用アカウントの対策	大会前に、**業務で利用しているアカウントのパスワードを1度変更**する。 ※業務用アカウントのパスワード変更を行う際は、業務影響を十分に考慮した上で実施するように注意が必要です。
	業務で利用している**アカウントを複数システムで使いまわしていないことを確認**する。
	利用されていない**不要なアカウントがないか確認**する。
大会前の最後の確認３．マルウェア等による被害の極小化	
４．不審なメールに対する対策	**不審なメールの添付ファイルは開かない、URLはクリックしない事を、大会前に今一度、組織内に周知**する。
	Wordの設定で**マクロの自動実行を無効化**する。
５．バックアップからのリカバリ方法の確認	**重要なデータが、**バックアップ対象となっており、**バックアップされていることを確認**する。
	バックアップされたデータから**復元する手順が用意されていることを確認**する。
	手順通りにデータを復元できるか確認する ※復元手順を確認する場合は、本番業務に影響が生じないよう注意が必要です。
大会前の最後の確認４．インシデント発生時の被害の極小化	
６．大会直前・大会期間中の重要システムの移行作業を控える	**大会直前・大会期間中**には、重要なシステムの**移行作業や急ぎでないセキュリティ更新作業等は可能な範囲で控える。**※既に計画されている作業について、すぐさま止めて頂く必要はありません。
	大会直前・大会期間中に重要なシステムの移行作業やセキュリティ更新を予定している場合は、**不具合が起きた場合にリカバリできるよう関係者で手順を確認**する。
７．システム構成の把握	基盤、ミドルウェア、アプリケーション、クラウドサービス等の**システムの構成状況を確認・把握**する。
	基幹サービスや業務環境の**ネットワーク構成を確認・把握**する。
８．大会に向けた気付きの強化	**大会直前・大会期間中**は、可能な範囲でサーバやアプリケーション等の**監視強化や、**セキュリティ機器等による**検知機会を増やすことができるか確認**する。