資料2

NISC National Information Security Center

重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針及び対策編の見直しについて

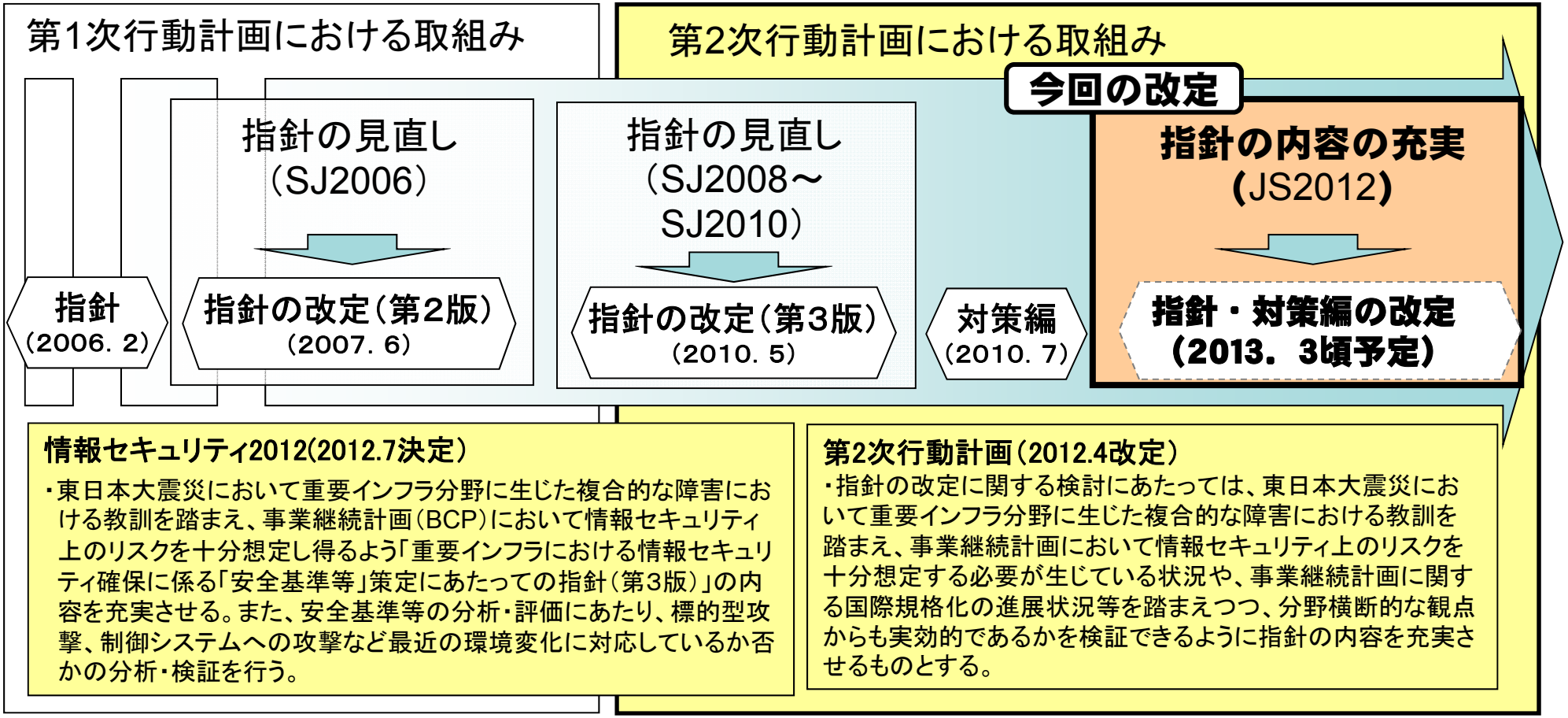
2012年 9月27日

内閣官房 情報セキュリティセンター（NISC）

「指針・対策編の見直し」の概要

○2010年度に、<u>指針（※1）の改定</u>（2010年5月）、<u>対策編（※2）の策定</u>（2010年7月）を行い、<u>各分野にて安全基準等の見直し</u>が順次行われているところ

○東日本大震災や標的型サイバー攻撃等の環境変化を受けた<u>第2次行動計画の改定</u>（本年4月）に伴い、<u>指針・対策編を分析・検証し、必要に応じて改定</u>を実施するとされたところ

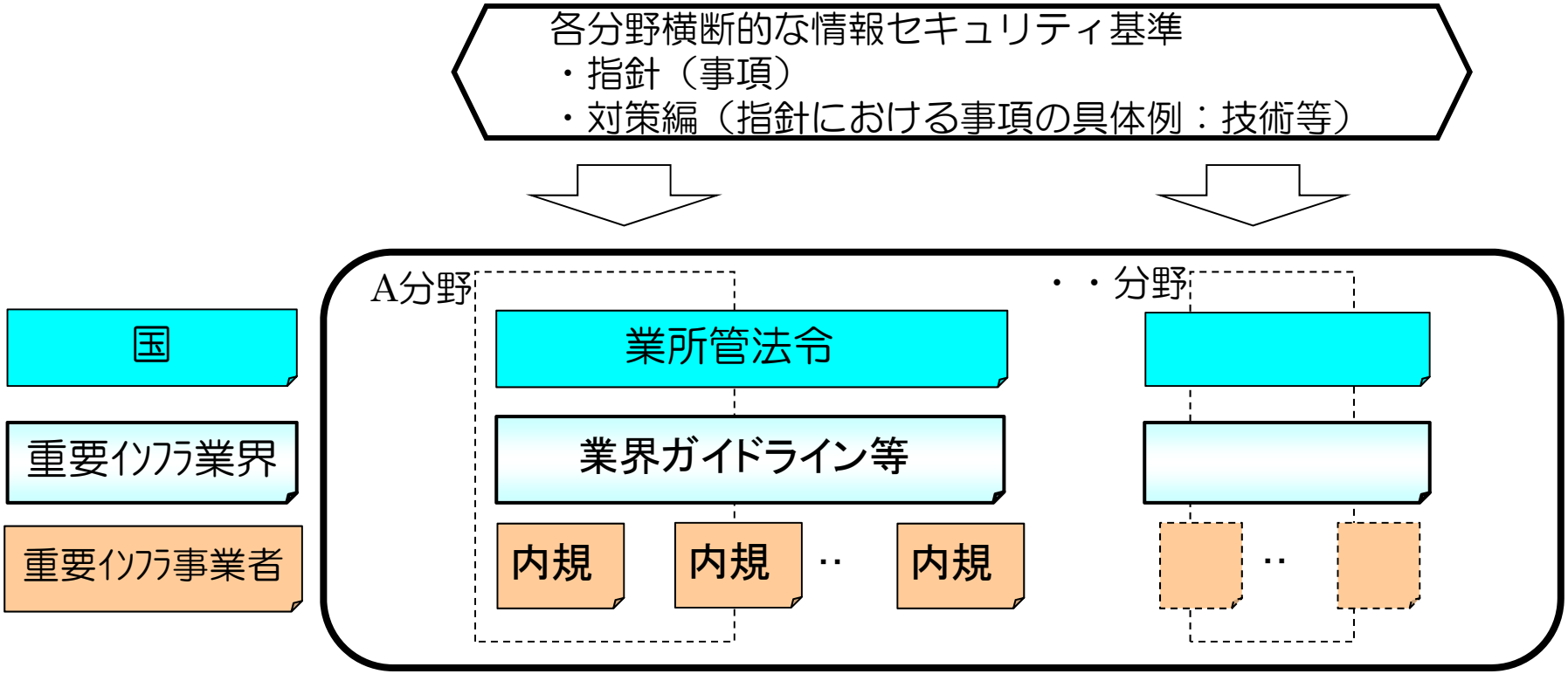


（※1）重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（情報セキュリティ政策会議決定）
（※2）重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針　対策編（重要インフラ専門委員会決定）

【参考】指針の位置づけ

＜指針＞

重要インフラ10分野における横断的な情報セキュリティ基準を定めたもの



【参考】重要インフラ第2次行動計画の改訂と具体的な対応

項目	行動計画の改訂	具体的な対応 （平成24年度）
1. BCP等の充実	BCP関連の記述を修正・追加 （Ⅱ　1.（1）指針の継続的改善）	**「安全基準等の策定に当たっての指針」または「対策編」に、通信途絶時の対策等IT－BCPに関する項目を追記**
2. 環境変化を踏まえた安全基準の改善	対策が求められる例として「標的型攻撃」、「制御システムへの攻撃」を追加 （Ⅱ　1.（2）安全基準等の継続的改善）	**攻撃の動向、情報システムの変化等の環境変化への安全基準の対応状況を精査※** ※必要に応じて「指針」または「対策編」に必要な項目を追加するとともに、国際標準に準拠した評価認証機関の活用またはセキュリティ検証施設の活用等制御システムのセキュリティ評価・検証を容易にするための方策を追加。
3. 情報共有体制の強化	重要インフラ事業者等と政府機関等の密接な意見交換や事業者にも役立つ情報の共有等、取組みを具体的に追加 （Ⅱ　2.（4）セプターカウンシル）	**セプターカウンシルにおいて、システムの運用状況の客観的判断材料等事業者間で共有可能な情報の追加を具体的に検討**

（第29回情報セキュリティ政策会議資料2-1より抜粋）

【参考】指針・対策編の策定・改定の経緯

年月	決定機関	名称	主な改定（追加）内容
2006年6月	情報セキュリティ政策会議	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第1版）	・重要インフラ分野内及び分野間の対策レベルの格差を最小限にし、統一的な重要インフラ防護に資する目的で、共通の指針を策定
2007年7月	情報セキュリティ政策会議	（第2版）	・自己点検・監査の実施 ・システムの負荷分散、冗長化 ・システムの処理性能確保、品質確保
2010年5月	情報セキュリティ政策会議	（第3版）	・IT障害発生時におけるサービス状況等の利用者への情報提供 ・新型インフルエンザ等の新たな脅威に対する対応 ・先進的な個別対策も取り込めるような記載
2010年7月	重要インフラ専門委員会	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針対策編（第1版）	・重要インフラ分野及び事業者が安全基準等を定めるにあたり、実践的な参考になるよう、具体例を記した「対策編」を策定

「指針・対策編見直し」の分析・検証におけるアプローチ

○今回の分析・検証においては、以下の3つの視点から検討が必要な課題を抽出し、指針・対策編への反映を検討する。

◆指針・対策編見直しの分析・検証における３つのアプローチ

①事業継続計画（BCP）の一層の充実：
「東日本大震災における重要インフラの情報システムに係る対応状況等に関する調査」（23年度）や複合的障害を想定した分野横断的演習での気づき・教訓を指針・対策編へ反映。

②標的型サイバー攻撃等の環境変化に対する対応：
標的型サイバー攻撃・制御システムへの攻撃への対策について、H23年度の共通脅威分析結果等を検証した上で、必要に応じて対応策を指針・対策編へ反映。

③他基準との平仄合わせ：
政府統一基準群に記載されている対応策について、比較検討の上、必要に応じて指針・対策編へ反映。

指針・対策編　2012年度改定（案）の方針

以下の3つの視点からのアプローチにより課題を抽出し、対応する対策を追記。

①業務継続計画（BCP）の一層の充実	（1）広域災害、複合障害を想定した対策を進めることを求める	指針本編
	（2）通信が途絶した中での緊急時行動ルールの策定を求める	対策編
	（3）通信途絶時の対策を追記	
	（4）停電への対応を追記	
	（5）代替手段で使用するシステムの準備を追記	
	（6）緊急時に使用が増加するシステムの準備を追記	
	（7）相互支援に備えたデータ形式の標準化推進を追記	
②標的型サイバー攻撃等の環境変化に対する対応	（1）ID・パスワード管理の強化策の詳細化	
	（2）入口対策の詳細化	
	（3）出口対策の詳細化	
	（4）ネットワーク構成等に関する情報の取扱いを追記	
	（5）モバイル端末のセキュリティ対策の詳細化	
	（6）グループ会社全体でのセキュリティ対策体制の整備を追記	
	（7）業界内、ベンダー等との情報連絡体制の構築を追記	
③他基準との平仄合わせ	（1）事業継続計画と情報セキュリティ対策の整合性確保を明記	
	（2）メールのなりすまし防止策を追記	
	（3）ID・パスワード管理の強化策の追記	

状況検証：①事業継続計画（BCP）の一層の充実（ 1/2 ）

東日本大震災における重要インフラの情報システムに与えた影響調査（平成23年度）及び分野横断的演習で得られた課題・気づきの検証を実施

	課題	検証結果
（1）広域災害、複合障害に対する対策	● 広域災害、複合障害を想定した対策を実施していなかった	● 広域災害、複合障害についても想定した事業継続性確保の個別対策の実施が望まれる
（2）緊急時の行動ルール	● 通信が途絶した状況で、意思決定する役割を持った経営層等との連絡がとれず、初動が遅れた	● 被災後の初動を早くするために、通信が途絶した状態でも、要員の参集や意思決定等の権限委譲が自動的に行われるような緊急時の行動ルールの策定が望まれる
（3）通信途絶時の対策	● 正副の通信回線が同時に切断され、通信回線が使用不可となった ● 固定電話・携帯電話は輻輳により使用できなかったが、衛星携帯電話・優先電話は使用できた ● 通信が途絶しても手元にデータを残していたため、必要最小限の業務ができた	● 通信回線の二重化や通信キャリアを正回線、副回線で分けるなど、同時被災しないような通信回線の対策が望まれる ● 輻輳などで一部の通信手段が使用できなくなる可能性を考慮し、複数の通信手段を準備し、使用できるようにしておくことが望まれる ● 通信途絶時でも必要最小限の業務ができるように準備しておくことが望まれる
（4）停電への対応	● 自家発電機の準備・訓練が不十分であったため、有効に使用できなかった ● 実際には発生しなかったが、自家発電機の燃料があと少しで枯渇した	● 災害時の停電に備えて自家発電装置等使用の準備・訓練と燃料対策を実施しておくことが望まれる

状況検証：①事業継続計画（BCP）の一層の充実（2/2）

	課題	検証結果
（5）代替手段で使用するシステムの準備	● 事務代行拠点からのアクセス権限付与を可能とする機能がなく、急きょ、システム変更を実施し、事務代行拠点からのアクセスを可能とした	● 災害時に代替手段として必要となるシステムを平時から開発し、準備しておくことが望まれる
（6）緊急時に使用が増加するシステムの性能の確保	● 利用者に重要サービスの提供状況等を発信する情報発信システム等、災害時に重要なシステムの可用性の確保が不十分であったため、アクセス集中により、サーバがダウンするなどの事象が発生	● 災害時に重要な機能を担う情報発信システム等の可用性を高めるため、平時から定期的にシステム性能を見直す等の対策を行うことが望まれる
（7）相互支援に備えたデータ形式の標準化	● 業界内で、データ形式が共通化できていなかったため、他の事業者が支援のために使用できなかった	● 災害時に業界内で相互支援できるように、データ形式の標準化を推進することが望まれる

反映の方向性：①事業継続計画（BCP）の一層の充実

分析・検証結果より抽出した問題意識	指針・対策編への反映の方向性	
①東日本大震災を踏まえた環境変化の検証より		
● 広域災害、複合障害を想定した対策の実施	● 本編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、考慮すべき脅威の例示等を追記。	（1）
● 通信が途絶した状態でも、要員の参集や意思決定等の権限委譲が自動的に行われるような緊急時のルール作り	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（2）
● 通信回線の二重化や通信キャリアを正回線、副回線で分けるなど、同時被災しないような通信回線の対策	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（2）
● 輻輳などで一部の通信手段が使用できなくなる可能性を考慮し、複数の通信手段を準備し、使用できるようにしておくこと	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（3）
● 通信途絶時でも必要最小限の業務ができるように準備しておくこと	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（3）
● 災害時の停電に備えて自家発電装置等使用の準備・訓練と燃料対策を実施しておくこと	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（4）
● 災害時に必要となる機能を平時から開発し、準備しておくこと	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（5）
● 災害時に重要な機能を担う情報発信システム等の可用性を高めるため、平時から定期的にシステム性能を見直す等の対策を行うこと	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（6）
● 災害時に業界内で相互支援できるように、データ形式の標準化を推進すること	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（7）

状況検証：②標的型サイバー攻撃等の環境変化に対する対応

共通脅威分析（平成23年度）の結果等から、対策課題の分析・検討を実施

	対策課題	分析結果
(1)ID・パスワードの管理	● 攻撃者にアクセス権限を容易に奪取されないように、ID・パスワードの管理を厳格化すべき	● 共用IDの禁止、不要IDの削除の徹底、IDごとに異なるパスワードを設定する等の対策の追加が必要と考える
(2)入口対策	● アンチウィルスソフトやIDS等だけではなく、多層的な防御対策が必要	● WAF（ウェブアプリケーションファイアウォール）や迷惑メールフィルターの導入、脆弱性のある作り込みをしないような対策等も必要と考える
(3)出口対策	● 侵入されても情報窃取を防ぐためには、外部への通信制御が重要	● 内部から外部への通信制御としてプロキシ経由にするなどの対策が必要と考える
(4)ネットワーク構成情報の管理	● 攻撃者にネットワーク構成等に関する情報が漏れないようにすべき	● ネットワーク構成等に関する情報の秘匿対策が必要と考える
(5)モバイル端末のセキュリティ対策	● モバイル端末が高度化する中、暗号化機能の実装だけでなく、ワンタイムパスワードや遠隔消去等の機能も必要	● ワンタイムパスワードや遠隔ロック、遠隔消去等の機能の実装も必要と考える
(6)グループ会社を含めた体制	● セキュリティ対策が十分でないところからの侵入を防ぐため、本体企業だけでなく、グループ会社も含めたセキュリティ対応が必要	● グループ会社も含めたセキュリティ対応体制の構築が必要と考える
(7)情報連絡体制	● 業界内、ベンダー等との情報連絡が重要	● 業界内、ベンダー等との、緊急時及び平常時の連絡体制の整備が必要と考える

反映の方向性：②標的型サイバー攻撃等の環境変化に対する対応

分析・検証結果より抽出した問題意識	指針・対策編への反映の方向性	
②標的型サイバー攻撃に対する対策の分析より		
● 共用IDの禁止、不要IDの削除の徹底、IDごとに異なるパスワードを設定する等の対策の追加	● 対策編：「4つの柱　ウ　情報セキュリティ要件の明確化に基づく対策」に、対策項目の例示等を記載。	（1）
● WAF（ウェブアプリケーションファイアウォール）の導入や脆弱性のある作り込みをしないような対策	● 対策編：「 4つの柱　ウ　情報セキュリティ要件の明確化に基づく対策」に、対策項目の例示等を記載。	（2）
● 内部から外部への通信制御としてプロキシ経由にするなどの対策	● 対策編：「 4つの柱　エ　情報システムについての対策」に、対策項目の例示等を記載。	（3）
● ネットワーク構成等に関する情報の秘匿対策	● 対策編：「 4つの柱　エ　情報システムについての対策」に、対策項目の例示等を記載。	（4）
● ワンタイムパスワードや遠隔ロック、遠隔消去等の機能の実装	● 対策編：「 4つの柱　エ　情報システムについての対策」に、対策項目の例示等を記載。	（5）
● グループ会社も含めたセキュリティ対応体制の構築	● 対策編：「 4つの柱　ア　組織・体制及び資源の対策」に、対策項目の例示等を記載。	（6）
● 業界内、ベンダー等との、緊急時及び平常時の連絡体制の整備	● 対策編：「5つの重点項目　ウ　外部委託における情報セキュリティ確保のための対策」に、対策項目の例示等を記載。	（7）

状況検証：③他基準との平仄合わせ

政府統一基準群に記載されている対応策について、指針・対策編との比較分析を実施

	対策	分析結果
（1）事業継続計画とセキュリティ対策の整合性	● 業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との整合性の確保、必要な措置の実施	● 事業継続計画と情報セキュリティ対策との間の整合性確保が重要インフラ分野にも必要と考える
（2）電子メールのなりすまし対策	● 電子メールの送信元について、なりすましの防止策を講ずる	● 電子メール送信時及び受信時の送信ドメイン認証の導入が重要インフラ分野にも必要と考える
（3）ID・パスワードの管理	● 攻撃者にアクセス権限を容易に奪取されないように、IDごとに異なるパスワードを設定する	● IDごとに異なるパスワードを設定することが重要インフラ分野にも必要と考える

反映の方向性：③他基準との平仄合わせ

分析・検証結果より抽出した問題意識	指針・対策編への反映の方向性	
③政府統一基準に記載されている対策の分析より		
● 事業継続計画と情報セキュリティ対策との間の整合性確保	● 対策編：「5つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に、対策項目の例示等を記載。	（1）
● 電子メール送信時及び受信時の送信ドメイン認証の導入	● 対策編：「４つの柱　エ　情報システムについての対策」に、対策項目の例示等を記載。	（2）
● IDごとに異なるパスワードを設定	● 対策編：「４つの柱　ウ　情報セキュリティ要件の明確化に基づく対策」に、対策項目の例示等を記載。	（3）

指針・対策編の改定に向けたスケジュール

○今後、各重要インフラ分野における意見を集約・反映し、来年1～2月頃のパブリックコメントを経て、今年末頃に指針・対策編の改定版を策定（指針については、政策会議で策定）

○本改定版は、安全基準等の継続的改善の際に活用されることを期待