統合開発クラウド マニュアル

管理者編
セキュリティガイドライン

第 1.0.3 版

2020 年 12 月 14 日

株式会社 NTT データ　システム技術本部

更新履歴

版数	改訂日	改定項目	改定内容	改定理由
1.0	2017/08/07	初版公開	第 1.0 版を公開	
1.0.1	2017/09/29	全章	[変更] 目次・誤字脱字の修正	記載誤りを修正
1.0.2	2020/06/30	1.1.本ガイドラインの目的と位置づけ 1.2.テナント管理者の責任範囲 2.4.ソフトウェア・サービスの利用制限 2.5.ウイルス対策	[変更] 誤字の修正	記載誤りを修正
1.0.3	2020/12/14	1.2.テナント管理者の責任範囲	[変更] 旧アクセス中継サービス提供終了に伴う修正	旧アクセス中継サービス提供終了に伴い、UDS アクセス中継サービスに記載内容を修正

目次

第 1 章　はじめに

1.1 本ガイドラインの目的と位置づけ

本ガイドラインは、テナント管理者が、統合開発クラウドのテナントに開発・テスト環境を構築する上で順守すべきセキュリティルールを示すものです。本ガイドラインの掲載ルールは、以下の 2 つの観点を基に「情報セキュリティポリシー（規程）」を初めとする NTT データの各種セキュリティルールのうち必要なルールを抽出し、引用したものであり、原則、順守が必要なものとなります。

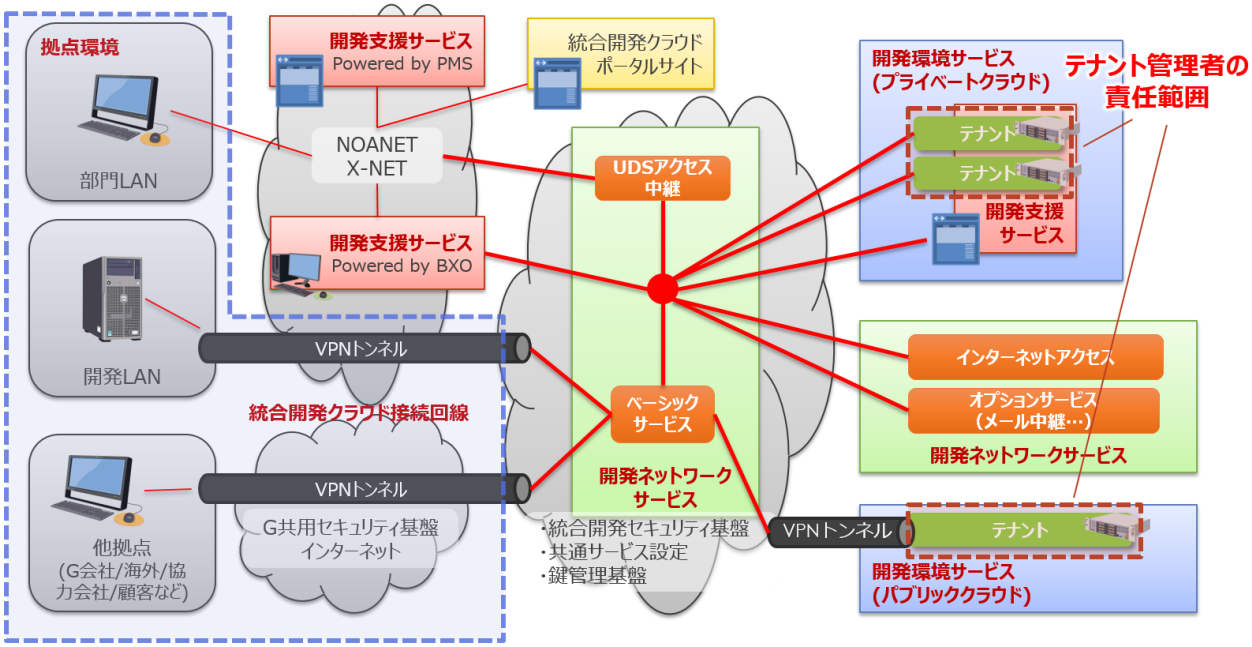
- **統合開発クラウドは、社内ネットワークにおける「開発 LAN[1]」上に存在するシステムとして、「社内ネットワークの構築／運用管理に関する実施方法」にて定めるセキュリティ対策を行う必要がある。**
- **開発プロジェクトとして、「ビジネスマネジメント実施方法（ライフサイクル編）」にて定めるセキュリティ対策を行う必要がある。**

[1] 部門ネットワークのうち、基幹ネットワークやインターネットにアクセス不可能な部分を言います。主にシステム開発や社外との情報共有を目的としています。

1.2 テナント管理者の責任範囲

テナント管理者は、図 1 の赤枠部分である「開発環境サービス（プライベートクラウド／パブリッククラウド）」上の「テナント」に対してセキュリティ確保の責任を持ちます。本ガイドラインは、この赤枠部分のセキュリティ確保に必要となるルールを掲載しています。

なお、図 1 の青枠部分である「拠点環境」や「統合開発クラウド接続回線」については、NTT データ、G 会社（国内・海外）、協力会社、顧客など各拠点の責任で、各々のルールに従いセキュリティを確保するものであり、本ガイドラインの対象とはしていません。



+

図 1 テナント管理者のセキュリティ確保に対する責任範囲

テナントのセキュリティ確保にあたっての基本事項として、情報は、指定された情報種別に基づき、情報の所有者・管理者・利用者がそれぞれの役割、責任、権利において情報を取り扱うものとします。（詳細は、「情報セキュリティポリシー（規程）」第 2 章 参照）

テナント管理者のセキュリティ管理対象は、図 2 に示す通り、テナント内仮想サーバの「OS 管理」や「テナント内ネットワーク管理」、「アプリケーション管理」、「テナント内ユーザー管理」、「アクセス管理」、および、「共通サービス設定要件」（DNS・Proxy 等の共通サービスに対する設定要件）があります。テナント管理者は、これらのセキュリティを確保する際に、本ガイドラインに掲載するルールを基にして対策を決定することになります。

図 2 テナント管理者のセキュリティ管理対象

1.3 本書の構成

本書は表 1 に示す通り、全 4 章から構成される。また、本書の見方を図 3 に示します。

表 1 本書の構成

章タイトル	概要
第 1 章 はじめに	本ガイドラインの目的や、テナント管理者の責任範囲等。
第 2 章 技術的対策	技術面のセキュリティ対策について提示する。
第 3 章 運用的対策	運用面のセキュリティ対策について提示する。
第 4 章 引用元ドキュメント	引用元ドキュメントの保管先について示す。

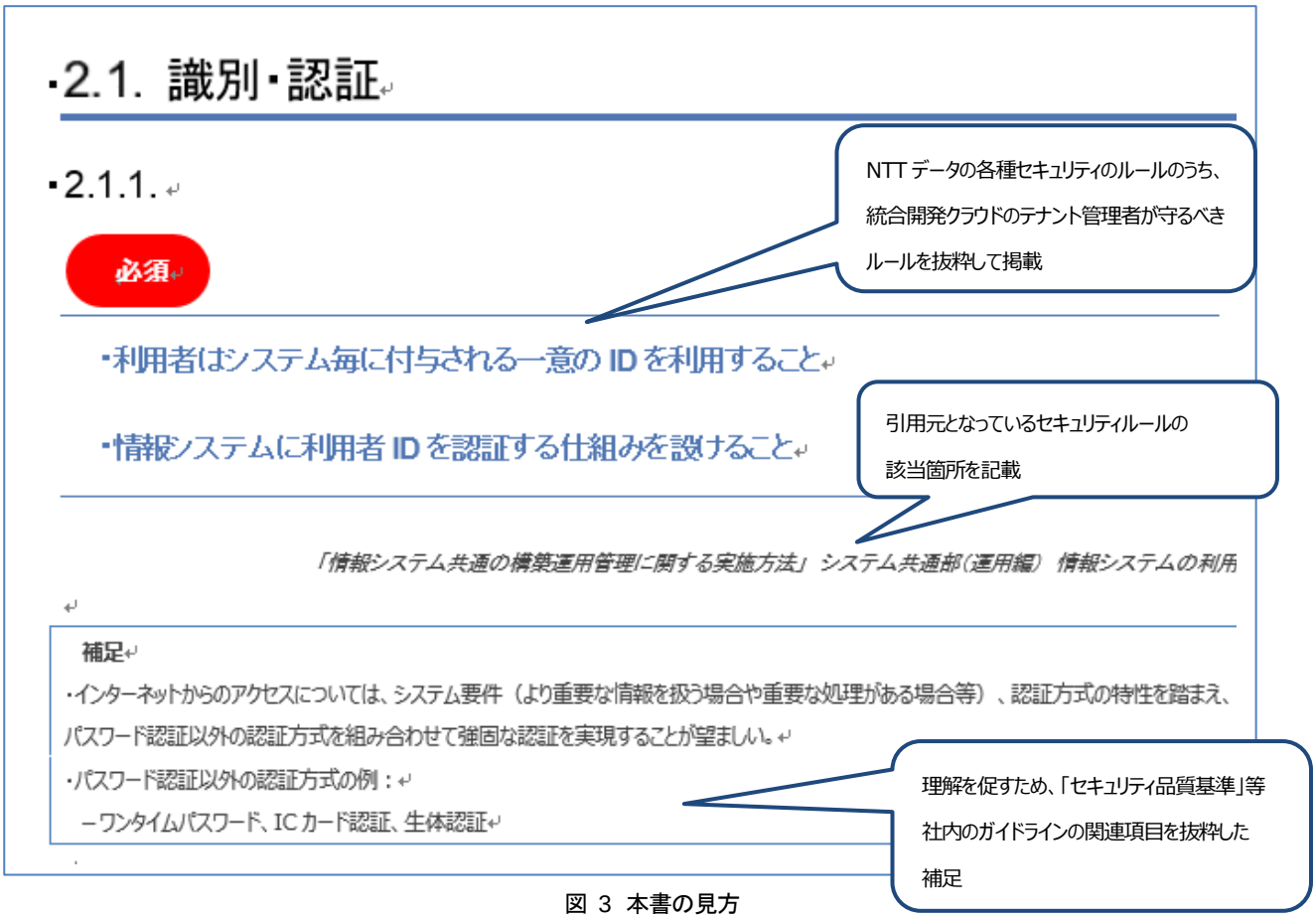


図 3 本書の見方

第 2 章　技術的対策

2.1. 識別・認証

2.1.1.

必須

・利用者はシステム毎に付与される一意の ID を利用すること

・情報システムに利用者 ID を認証する仕組みを設けること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（運用編） 情報システムの利用

補足

・インターネットからのアクセスについては、システム要件（より重要な情報を扱う場合や重要な処理がある場合等）、認証方式の特性を踏まえ、パスワード認証以外の認証方式を組み合わせて強固な認証を実現することが望ましい。

・パスワード認証以外の認証方式の例：

－ワンタイムパスワード、IC カード認証、生体認証

2.1.2.

必須

一定時間操作が無い場合、自動ロックされるよう設定すること

「記録媒体内蔵機器取扱い実施方法」 第6章 仮想PCの取扱い 第1節 技術的対策

補足

・一定時間は 5 分間以下とすることが望ましい。

・システムの業務要件に合わせて適切な時間を設定すること。

・ロックは、セッションロック（アカウントロック）もしくは画面ロック（復帰時にパスワードの入力が必要なタイプ）を指している。システム管理者利用者の操作環境（入退室管理の実施状況、リモート接続有無等）等に応じて、方法を検討すること。

2.1.3.

強く推奨

ログインに失敗した場合に表示するエラーメッセージは、認証に失敗した理由が ID か認証パスワードかを特定できないエラーメッセージとすること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足

・エラーメッセージの違いにより、ID の存在が判明し、攻撃者に悪用される恐れがある。

・同様に、アカウントロックした場合に表示するエラーメッセージについても、アカウントロックしたことや ID/認証パスワードが正しいことが分からないメッセージとするのが望ましい。ただし、ユーザーの利便性を確保するために、アカウントロックした場合はあらかじめ登録されたユーザーのメールアドレスへ、アカウントロックした旨を通知する等の対応もあわせて検討すべきである。

2.1.4.

強く推奨

認証パスワードは、不可逆暗号化（ハッシュ化）したうえで保存すること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足

・不可逆暗号化（ハッシュ化）は、パスワード（平文）の情報を秘匿するための対策。

・不可逆暗号化（ハッシュ化）されたハッシュ値が漏洩した場合に、繰り返し任意の文字列をハッシュ化しハッシュ値と比較することで、パスワードの平文を解析する攻撃が考えられる（レインボーアタック）。その対策としてシステム利用者ごとに異なる文字列を付与してから不可逆暗号化（ハッシュ化）することで、解析を困難にする対策がある。付与する文字列はソルト（salt）と呼ばれ、ソルトの例として、ID を入力とした関数や、乱数を用いる方法がある。

・認証パスワードをシステムに保存しない認証方式（例：OTP）については、認証パスワードの保存時の不可逆暗号化（ハッシュ化）は対象外。

2.1.5.

強く推奨

情報システム利用者及び情報システム管理者のパスワードを変更できる環境を提供すること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（運用編） システム管理（Ｉ）サーバアクセス制御

補足

・なし

2.1.6.

強く推奨

認証パスワードやクレジットカード番号を画面表示および帳票印刷する際には、"＊"に置き換える等、非表示にすること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-2.アクセス制御

補足

・ショルダーハッキングの防止策、及び帳票からの情報漏えい対策。

・認証パスワードは入力画面も含めすべて"*"等に置き換える、もしくは非表示とすること。

・PCIDSS では、クレジットカード番号について、最初の 6 桁と最後の 4 桁を最大表示桁数とし、それ以外の数字は"*"等に置き換えるもしくは非表示とすることとしている。ただし、入力画面については表示しても構わない。

・認証パスワードやクレジットカード番号は、画面表示だけではなく、HTML ソースにも含めないこと。

2.1.7.

推奨

他者に認証パスワードを勝手に変更されることを防ぐため、認証パスワードの変更において、変更前のパスワードと変更後のパスワードを（同じ画面で）入力させるようにすること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足

・なし

2.2. 特権管理

2.2.1.

必須

管理権限は、システム管理者のアカウントに、必要最小限付与すること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・特権アカウントの利用は最小限とし、通常運用では特権アカウントではないアカウントを使用すること。

・内部に侵入されることを前提に、特に管理権限やアカウントの細分化を含めて検討すること。

・ユーザーとシステム管理者のアカウントを分離し、ユーザーカウントに管理権限を割り当てないこと。

・システム管理者のアカウントにも、不必要な権限を割り当てないこと。

2.2.2.

推奨

システム管理者の管理権限を行使できる端末を制限すること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・ドメイン管理の権限を必要とする作業は、運用管理専用のセグメントからのみできるようにすること。

・内部ユーザー端末上から、システム管理者アカウントを行使する場合、必要のない操作ができないようにすること。

2.2.3.

推奨

・特権 ID は利用者 ID とは異なる ID を付与すること

・情報システムに特権 ID を認証する仕組みを設けること

・情報システムに特権 ID の利用者が特定できる仕組みを設けること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（運用編） システム管理（Ⅰ）サーバアクセス制御

補足

・なし

2.3. アクセス制御

2.3.1.

必須

掲載情報の情報種別に応じた認証・アクセス制御機能を有していること

「ホームページの構築運用管理に関する実施方法」 Webサーバ構築・管理 Webサーバ構築

補足

・アクセス制御方法の例：

－システム利用者の役割（利用者・管理者・代行者・作業者等）を明確に規定し、閲覧可能な情報を制限する。

－認証後にのみ閲覧可能なコンテンツ（HTML ファイル、画像、ドキュメントファイル等）への URL やパラメータを、直接入力、変更されても閲覧できないようにする。

－時間帯や曜日によってアクセス可能な機能や処理量を制限する。

－CGI、ASP プログラム等のスクリプトを配置するディレクトリを限定する。

・DBMS の管理権限、DBMS のテーブルや各種ファイルのアクセス権限、VM 毎のシステム管理権限、保守運用に必要なアクセス権限等を明確に規定して制限することが望ましい。

・システム管理者による不正行為が行われないように、システム管理の手順は、一人に権限を集中させないとともに、一人作業の禁止等により夜間休日の監視の目が甘くなる時でも不正行為が行えないような処置を講じること。

・ID 管理と権限管理は分離することが望ましい。

・各種サービスの運用のために用いられるシステムアカウントについてもアクセス制御を行うこと。特に、AP、DB 間のアクセスについては、特権アカウントのまま AP からフルアクセス可能な設定となっているケースが見られる。

2.3.2.

必須

共有ファイルは情報種別に応じたアクセス制御を実施し、必要に応じて暗号化すること

「共有ファイルシステムの構築／運用管理に関する実施方法」 利用 格納するファイル

補足

・アクセス制御に関しては 2.3.1 の補足を参照。

2.3.3.

強く推奨

システム内に設置した NW 機器（ファイアウォール、ルータ、スイッチ、ロードバランサ等）、ミドルウェア（データベース製品、AP サーバ等）の管理機能に対しては、最低限のアクセスのみを許可すること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-2.アクセス制御

補足

・第三者が管理機能に不正にアクセスできないようにするための対策。

・管理機能に対するアクセス制御の例：

– 管理セグメントを設置したうえで、管理セグメントからのアクセスのみを許可する。

– 接続元 IP アドレスによってフィルタリングを行う。

2.3.4.

強く推奨

システム管理者によるアクセスは、システム内もしくは閉域ネットワーク経由のみに制限すること

「記録媒体内蔵機器取扱い実施方法」 第6章 仮想PCの取扱い 第1節 技術的対策

補足

・閉域ネットワークとは、システム管理に無関係な者が物理的かつ論理的にアクセスできないネットワークを指している。専用線や IP-VPN は閉域ネットワークに含まれるが、インターネット VPN は含まれない。

・システムの管理権限を悪用された場合、システムの乗っ取り等、想定されるセキュリティリスクは大きい。そのため、攻撃を受ける機会を減らすた

めに、システム管理者がアクセスできるルートはシステム管理に無関係な者がアクセスできないようにすべきである。

・IDS/IPS 等の監視用のトラフィックは、システム管理者によるアクセスとはみなさない。

2.3.5.

推奨

業務上必要のない、端末のファイル共有を制限すること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・なし

2.3.6.

推奨

共有ファイルに必要最小限のアクセスコントロールリストを設定すること

「共有ファイルシステムの構築／運用管理に関する実施方法」 運用 アクセスコントロールリストの設定及び更新

補足

・なし

2.4. ソフトウェア・サービスの利用制限

2.4.1.

必須

インストールするソフトウェア/起動するサービス・機能は、業務上必要最小限とし、インストール/有効化している理由を明確にすること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・NW 機器についても不要な機能、サービス、ポートは停止することが望ましい。
（例えば、メンテナンスを CUI のみで行うのであれば、管理コンソールは不要であるため停止する等）
・業務上必要のないコマンドやスクリプトの起動ができないようにすること。
・コマンドやスクリプト起動停止の例：
－メールサーバにおいて、VRFY および EXPN コマンド並びにその他の不要な管理コマンドを停止する
－端末において業務上必要のないコマンドやスクリプトの起動ができないようにする

2.4.2.

必須

必要最小限のデーモン、プロセスのみを起動すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 外部接続環境のセキュリティ要件

補足

・なし

2.5. ウイルス対策

2.5.1.

必須

・ウイルス対策ソフトをインストールすること

・ウイルス定義ファイルを最新化すること

・リアルタイム保護機能を有効化すること

・ウイルス検査を定期的に実施すること

「記録媒体内蔵機器取扱い実施方法」第6章 仮想PCの取扱い 第1節 技術的対策

補足

・内部ユーザーの全端末に対し、ウイルス対策ソフトを導入すること。

・システムを構成する Windows® operating system（端末、サーバ）には、すべてウイルス対策ソフトを導入すること。

・導入対象を検討する際には、性能への影響が許容可能かも考慮すること。

・ウイルスの侵入経路で漏れがないようにとは、ウイルスが侵入する可能性のある経路が複数ある場合に、その複数の経路を漏れなくという意図である。必ずしも経路上にある全ての構成要素にウイルス対策ソフトを導入することを意図するものではない。

2.5.2.

必須

・情報システム利用者は、外部から取得したファイル及び共用するファイル媒体の利用前にウイルス検査を実施すること

・情報システム利用者は、出所不明のソフトウェアを使用しないこと

・情報システム利用者は、ウイルス検出時は、ウイルス対策責任者に報告すること

・情報システム利用者は、ファイルを他者へ提供する際は、事前にウイルス検査を実施すること

「情報システム共通の構築運用管理に関する実施方法」システム共通部（運用編） コンピュータウィルス

補足

・内部ユーザーの全端末に対し、ウイルス対策ソフトを導入すること。

・システムを構成する Windows® operating system（端末、サーバ）には、すべてウイルス対策ソフトを導入すること。

・導入対象を検討する際には、性能への影響が許容可能かも考慮すること。

・ウイルスの侵入経路で漏れがないようにとは、ウイルスが侵入する可能性のある経路が複数ある場合に、その複数の経路を漏れなくという意図である。必ずしも経路上にある全ての構成要素にウイルス対策ソフトを導入することを意図するものではない。

2.5.3.

必須

ウイルス対策ソフトによるウイルス等検知の動作確認を行う場合は、実際のウイルス等を使用してはならない。動作確認を行う必要がある場合は、無害なテスト用ウイルス（eicar.com 等）を使用する

「ウイルス対策実施方法」侵入予防措置

補足

・なし

2.5.4.

必須

外部から取得したファイル及びソフトウェアを初めて使用する場合には、ウイルス対策ソフトによりウイルスチェックを行ってから使用する

「ウイルス対策実施方法」侵入予防措置

補足

・なし

2.5.5.

必須

不正プログラム対策ソフト（ここではウイルス対策ソフトを指す）において、不正プログラム検知時の通知先は、通知を随時確認できる通知先を設定すること

「セキュリティ品質基準」3.特有の攻撃パターンに対する対策 3-1.不正プログラム対策

補足

・通知先の例：

－システム管理用端末やコンソールの画面上

－システム管理者のメールアドレス

－システム管理者の常駐先に設置したパトランプ

2.5.6.

推奨

以下の条件を満たした場合、ウイルス対策ソフトを PC 等にインストールせず、ウイルス対策ソフトと他ソフト等との相性の動作調査を行うことができる

・調査開始前に、該当 PC 等内の全ファイルのウイルスチェックを行う。

・調査開始前に、該当 PC 等に最新のセキュリティパッチを適用する。

・調査中に該当 PC 等以外とのファイルの入出力は行わない。

・独立 LAN を除く社内ネットワークへの接続は、調査中は可能な限り短時間とする。

・調査中にウイルス等の侵入又は感染が疑われた場合は、即座に調査を中止し、ネットワークから切り離す。

「ウイルス対策実施方法」 侵入予防措置

補足

・なし

2.6. 暗号化

2.6.1.

強く推奨

次の箇所で使用している暗号アルゴリズムおよび鍵長は、十分な強度の暗号アルゴリズムおよび鍵長を使用すること

・システム外とやり取りする情報の暗号化、ハッシュ化（オンライン、オフライン問わず）

・認証パスワードのハッシュ化

「セキュリティ品質基準」1.基本的なセキュリティ機能 1-3.暗号

補足

・不十分な強度の暗号アルゴリズム/鍵長や第三者によって安全性が証明されていない暗号アルゴリズム/鍵長を使用した場合、暗号解読される可能性が高くなる。また、第三者によって安全性が証明されている暗号アルゴリズムを使用する場合でも、暗号アルゴリズムは危殆化するため、留意すること。

・十分な強度の暗号アルゴリズムおよび鍵長は、以下の最新情報を調査の上決定すること。

－CRYPTREC の電子政府推奨暗号リストに載っているもの

－NTT 持株の暗号危殆化対策マニュアル（技術方針）で使用を認めているもの

－NIST が使用を認めているもの

（上記情報の掲載先はセキュリティ品質基準（本編）3 章「1-3.暗号」(1)参考資料を参照）

2.6.2.

推奨

公開鍵暗号方式の秘密鍵、共通鍵暗号方式の共通鍵は、安全な方法で配付すること

「セキュリティ品質基準」1.基本的なセキュリティ機能 1-3.暗号

補足

・対象とする秘密鍵/共通鍵の例：

－通信路の暗号化（HTTPS 以外）に使用する共通鍵

－データや媒体の暗号化に使用する共通鍵

－クライアント認証に使用する秘密鍵

・安全な配付方法の例：

－IC カード等の耐タンパ製品による配付

－開封有無が分かる形式（封印シールの貼付等）での読み取り専用の媒体による配付

－封書、圧着ハガキによる配付

・秘密鍵・共通鍵と、それを保護したパスフレーズは、別々に配付すること。

・郵送する場合は、送達確認できる方法で配付すること。

2.6.3.

推奨

公開鍵暗号方式の秘密鍵、共通鍵暗号方式の共通鍵の紛失/漏えいが発生した場合に備え、秘密鍵、共通鍵の無効化、および新しい鍵への更新ができるようにすること

「セキュリティ品質基準」1.基本的なセキュリティ機能 1-3.暗号

補足

・対象とする秘密鍵/共通鍵の例：

– 通信路の暗号化（HTTPS 含む）に使用する秘密鍵/共通鍵

– データや媒体の暗号化に使用する秘密鍵/共通鍵

– 配布プログラムへの署名に使用する秘密鍵

– クライアント認証に使用する秘密鍵

・例えば、無効化する鍵で暗号化されていたデータがある場合、無効化する前に当該データを復号しておく手順の考慮が必要である。

第 3 章　運用的対策

3.1. セキュリティの基本事項

3.1.1.

必須

協働者が業務遂行に必要となる利用権限を明確にし、職務遂行の範囲内で使用すべき旨を指導したうえで権限を付与すること

「情報セキュリティポリシー（規程）」 第6章 情報セキュリティポリシーの運用 第11節 協働者に対する業務委託

補足

・特権アカウントの利用は最小限とし、通常運用では特権アカウントではないアカウントを使用すること。

・DBMS の管理権限、DBMS のテーブルや各種ファイルのアクセス権限、VM 毎のシステム管理権限、保守運用に必要なアクセス権限等を明確に規定して制限することが望ましい。

・システム管理者による不正行為が行われないように、システム管理の手順は、一人に権限を集中させないとともに、一人作業の禁止等により夜間休日の監視の目が甘くなる時でも不正行為が行えないような処置を講じること。

・ID 管理と権限管理は分離することが望ましい。

・各種サービスの運用のために用いられるシステムアカウントについてもアクセス制御を行うこと。特に、AP、DB 間のアクセスについては、特権アカウントのまま AP からフルアクセス可能な設定となっているケースが見られる。

3.1.2.

推奨

情報システム利用権限を貸与する場合は、「情報セキュリティポリシー（規程）」等の周知及び教育を実施すること

「情報セキュリティポリシー（規程）」 第3章 情報システム 第1節 情報システム利用の許諾

補足

・なし

3.1.3.

推奨

情報システムを構成するサーバ類を一意に識別するための識別子を付与すること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（構築編） サーバ設定（Ⅱ）命名規則等について

補足

・なし

3.1.4.

推奨

情報システム単位に、部門長は情報システム責任者を任命し、情報システム責任者は情報システム管理者を任命すること

「情報システム共通の構築運用管理に関する実施方法」 運用管理体制 役割等（Ⅰ）責任者、管理者の設置

補足

・なし

3.1.5.

推奨

情報システムを開発・改修する際はセキュリティ要件を明確化し、実装へ反映すること

「情報セキュリティポリシー（規程）」 第3章 情報システム 第6節 情報システムの開発・調達

補足

・なし

3.1.6.

推奨

情報システムの利用目的、利用対象者、利用期間を明確にすること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（構築編） システム構築時の整理

補足

・なし

3.1.7.

推奨

社内ネットワーク利用条件を満たす者に対してのみ、ネットワーク利用資格を貸与すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの利用資格 利用資格の貸与

補足

・なし

3.1.8.

推奨

プロジェクト終了後、速やかに不要となった開発ネットワークを撤去すること

「情報セキュリティポリシー（規程）」 第5章 プロジェクトのセキュリティ管理 第5節 開発ネットワーク

補足

・なし

3.1.9.

推奨

情報システムの構築・廃止にあたり、主管部門の部門長の承認を得ること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（構築編） システム構築・廃止の判断

補足

・なし

3.1.10.

推奨

・社員及び協働者が離任する際は、開示情報を廃棄・返却させること

・社員及び協働者が離任する際は、離任後も継続する機密保持に関する念書を取得すること

「情報の取扱いに関する細則」 6.情報の廃棄 情報の廃棄要領

補足

・認証情報の流出や不適切なアクセス権限の設定によるセキュリティインシデントを防止するための対策。

・システムに対して大きな権限を持つ Administrator や root アカウントのような特権アカウントについては、特に厳しく管理すること。

・管理簿を作成し管理することが望ましい。

・ドメイン管理のための識別認証情報が不正に使用されないように適切に管理すること。

・異動・離職時の対応としては、識別認証情報を削除するとログの監査/監視におけるシステム利用者の識別が困難となる場合、無効化することが望ましい。

・ユーザーの識別認証情報の管理ルールの例：

– ユーザーの識別認証情報を登録、更新、初期化、削除する際は、作業者とは別の者に承認を受け、必ず作業記録を残すこと。

– 有効期限を経過したアカウントは無効化すること。

– ユーザーがアクセス可能な情報は、業務上必要最小限の情報に限定すること。

– 作業記録は最低 3 年間は保存すること。

3.2. ID・パスワード管理

3.2.1.

必須

認証に使用するパスワードは複雑さの要件を満たす推測困難なものを設定し、半年に 1 回以上変更すること

「記録媒体内蔵機器取扱い実施方法」 第6章 仮想PCの取扱い 第1節 技術的対策

補足

・容易に推測されないためには、最小文字長と文字種について以下のように制限することが望ましい。

– 最小文字長：8 文字以上

－少なくとも含む文字種：英大文字、英小文字、数字、記号の中から 3 種類以上
・アカウントが突然ロックされることを防ぐため、有効期限が切れる前に、有効期限間近である旨を通知することも合わせて検討するとよい。
・再使用を禁止する期間もしくは個数を次の値に制限することが望ましい。
－パスワード再使用禁止期間：パスワード有効期限×4 以上
－パスワード再使用禁止個数：直近 4 個以上

3.2.2.

強く推奨

一定回数以上連続して認証に失敗した場合、システム利用者のアカウントをロックすること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足
・ブルートフォース攻撃等によるパスワード解析を防止するための対策。
・許容する連続認証失敗回数は、システムの運用条件にもよるが、「6 回以下」とすることが望ましい。PCIDSS においても「6 回以下」と規定している。
・ユーザーがアカウントロックされた場合、システム管理者による手動解除、もしくは、一定時間経過後に自動解除すること。自動解除を行う時間は、30 分以上とすることが望ましい。PCIDSS においても「30 分以上」と定めている。
・サポートデスク等でロック解除の運用を行う場合など、自動解除が不要な場合は、自動解除機能を設けないこと。
・システム管理者がアカウントロックされた場合、他のシステム管理者による手動解除を必要とすること。

3.2.3.

強く推奨

認証パスワードを変更できる役割を制限すること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足

・ユーザーの認証パスワードは、認証パスワードの所有者もしくは当該ユーザーを管理する役割のみが変更できるように制限すること。

・システム管理者の認証パスワードは、認証パスワードの所有者もしくは他のシステム管理者のみが変更できるように制限すること。

3.2.4.

強く推奨

OS/PP のデフォルトアカウントのパスワードは、すべて変更すること

「セキュリティ品質基準」2.構成要素の脆弱性に対する対策 2-2.システム基盤層の脆弱性対策

補足

・デフォルトアカウントのパスワードは、第三者に推測容易なパスワードである。

・デフォルトアカウントのパスワードの例：

－NW 機器のデフォルトアカウントのパスワード

－OS のデフォルトアカウントのパスワード

－PP（DBMS 等）のデフォルトアカウントのパスワード

・また、デフォルトアカウントのパスワードと同様、SNMP コミュニティ名についても変更するのが望ましい。

・可能であれば、デフォルトアカウント名を変更もしくは無効化する方がよい。

3.2.5.

強く推奨

端末のローカル管理者 ID とパスワードの組が複数の端末で同一とならないようにすること

「セキュリティ品質基準」4.システムの管理面での対策

補足

・端末のローカル管理者 ID とパスワードが同一の組になる例としては、複数の端末を構成する際に、同一のシステムイメージを複製する場合が挙げられる。このような場合、初期設定 ID/パスワードが同一となるため、端末利用開始前に変更されるようにすること。

3.2.6.

強く推奨

不要になったID及びアクセス権限は速やかに削除し、その記録を残すこと

「情報セキュリティポリシー(規程)」 第4章 アクセス制御 第1節 識別・認証

補足

・異動・離職したシステム管理者のアカウントの不正利用(異動したシステム管理者による不正利用も含む)を防止するための対策。

・ログをさかのぼって監査するときのことを考慮し、一定期間アカウントは削除せずに無効化すること。

・異動、離職が判明してから無効化を行う期限については、あらかじめルール化しておくことが望ましい。

3.2.7.

強く推奨

利用者アカウントを定期的に棚卸しすること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 リモートアクセス環境のセキュリティ要件

補足

・アカウント管理の漏れを防ぐため、定期的にアカウントの棚卸しを行うことが望ましい。（棚卸しルールについては他項目も参照。）

3.2.8.

強く推奨

有効なアカウントは、サービス提供に必要最小限のアカウントとし、有効にしている理由を明確にすること

「セキュリティ品質基準」 2.構成要素の脆弱性に対する対策 2-2.システム基盤層の脆弱性対策

補足

・Web サーバ等のサービス実行用のアカウントは、ログインを無効化すること。

・不特定多数が利用可能な共用アカウント(guest、demo 等)、デフォルトアカウントを無効化すること。

3.2.9.

推奨

情報システムの認証に生体認証を用いる場合は、登録データを個人情報として取り扱うこと

「情報セキュリティポリシー(規程)」 第4章 アクセス制御 第1節 識別・認証

補足

・なし

3.2.10.

推奨

利用者にグループ ID を付与する場合は、グループ ID の利用者を明確にすること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部(運用編) システム管理(Ⅰ)サーバアクセス制御

補足

・なし

3.2.11.

推奨

ID、パスワードの管理手順を定めること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（運用編） システム管理（Ⅰ）サーバアクセス制御

補足

・認証情報の流出や不適切なアクセス権限の設定によるセキュリティインシデントを防止するための対策。

・システムに対して大きな権限を持つ Administrator や root アカウントのような特権アカウントについては、特に厳しく管理すること。

・管理簿を作成し管理することが望ましい。

・ドメイン管理のための識別認証情報が不正に使用されないように適切に管理すること。

・異動・離職時の対応としては、識別認証情報を削除するとログの監査/監視におけるシステム利用者の識別が困難となる場合、無効化することが望ましい。

・ユーザーの識別認証情報の管理ルールの例：

－ユーザーの識別認証情報を登録、更新、初期化、削除する際は、作業者とは別の者に承認を受け、必ず作業記録を残すこと。

－有効期限を経過したアカウントは無効化すること。

－ユーザーがアクセス可能な情報は、業務上必要最小限の情報に限定すること。

－作業記録は最低 3 年間は保存すること。

3.2.12.

推奨

他者に認証パスワードが知られないよう、システム利用者に対して次の注意喚起を行うこと

・認証パスワードには次のような文字列を設定しないこと

－アカウント名または名前（意味のある一部も含む）

－辞書にある単語、生年月日

－上記の単純な組み合わせ

－上記と数字の単純な組み合わせ

・ID/認証パスワードを他者に教えないこと

・他のサービスと同じ認証パスワードを設定しないこと

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-1.識別認証

補足

・その他に注意喚起に含める事項の例：

－他者が容易に知りうる方法で管理しないこと（付箋に書いてディスプレイに張る等しないこと）

－システム管理者を偽ってパスワードを聞き出す詐欺行為に留意すること（システム側からパスワードをメールや電話で聞くことはない等の説明を行う）

・システム管理者の認証パスワードの場合、上記に加え以下についても注意喚起すること。

－ 認証パスワードには、会社名やシステム名等、容易に推測できる文字列を設定しないこと。

－ 他の用途で用いているパスワードの使いまわしを行わないこと。

・上記の「注意喚起」を、システムの利用画面で表示することも有効である。その場合は設計（画面設計）に反映すること。

3.3. 構成管理・変更管理

3.3.1.

必須

情報システムを構成するサーバに影響するサーバのパッチ情報とパッチ適用を入手し、対処すること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（運用編）セキュリティパッチ

補足

・セキュリティパッチは、当該パッチの一次配布元等の信頼できるところから収集すること。

・セキュリティパッチの適用要否を判断するための参考情報例：

－Security News Flash （G 外秘）のリスク表示
－JVN の脆弱性分析結果
－JVN iPedia の CVSS による深刻度
・セキュリティパッチの自動適用機能がある場合、意図しないセキュリティパッチが適用されることによるリスクを考慮の上、利用するか検討すること。
・内部ユーザーの端末は、セキュリティパッチの自動適用機能を利用することが望ましい。
・システムのバックアップが可能な機器についてパッチ適用後にバックアップを取得すること。ただし、システムバックアップを取得できないシステムは、前回バックアップを取得した時点から今回までに適用したパッチ、設定を再現できるよう管理しておくこと。

3.3.2.

必須

セキュリティパッチの適用によってシステムが想定外の動作をしないか確認するために、本番環境適用前に検証すること

「セキュリティ品質基準」 2.構成要素の脆弱性に対する対策 2-2.システム基盤層の脆弱性対策

補足
・検証の結果および適用可否の判断根拠の記録を残すこと。
・開発環境において検証し結果を本番環境に適用できるようにすること。

3.3.3.

強く推奨

セキュリティパッチの適用方法について、次の項目を文書化すること

・セキュリティパッチの収集先、収集タイミング

・セキュリティリスク評価、適用判断手順

・セキュリティパッチ適用タイミング

・内部ユーザーへの周知方法

「セキュリティ品質基準」 2.構成要素の脆弱性に対する対策 2-2.システム基盤層の脆弱性対策

補足

・セキュリティパッチは、当該パッチの一次配布元等の信頼できるところから収集すること。

・セキュリティパッチの適用要否を判断するための参考情報例：

－Security News Flash （G 外秘）のリスク表示

－JVN の脆弱性分析結果

－JVN iPedia の CVSS による深刻度

・セキュリティパッチの自動適用機能がある場合、意図しないセキュリティパッチが適用されることによるリスクを考慮の上、利用するか検討すること。

・内部ユーザーの端末は、セキュリティパッチの自動適用機能を利用することが望ましい。

・システムのバックアップが可能な機器についてパッチ適用後にバックアップを取得すること。ただし、システムバックアップを取得できないシステムは、前回バックアップを取得した時点から今回までに適用したパッチ、設定を再現できるよう管理しておくこと。

3.3.4.

強く推奨

各機器のソフトウェア構成、バージョン、セキュリティパッチの適用状況、サポート期間、依存関係を把握しておくこと

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・定期的に棚卸しを行うこと。

・システムライフサイクルに対し十分なサポート期間のあるソフトウェアを使用すること。

・不要な機器やソフトウェアを速やかに撤去、又は削除の上、構成情報を最新化すること。

・人手による運用だけではソフトウェアの最新バージョンやパッチの適用管理の徹底が難しい場合に、バージョン管理ソリューションを導入すること。

バージョン管理ソリューションの例：NOSiDE Inventory Sub System （検疫 NW・PC セキュリティ管理・PC 資産管理）

3.3.5.

推奨

情報システム種別の付与された情報システムに対して、変更管理手続を定めて変更管理を実施すること

「情報セキュリティポリシー(規程)」第3章 情報システム 第2節 情報システム責任者

補足

・なし

3.3.6.

推奨

・システム変更前に、その変更によるセキュリティリスクの有無を判断すること

・セキュリティリスクが有ると判断した場合には、その影響を分析すること

「セキュリティ品質基準」4.システムの管理面での対策

補足

・セキュリティリスクの有無の判断、および分析においては、機密性・完全性・可用性・真正性・責任追跡性・否認防止・信頼性の観点で検討する。

・分析結果および根拠や、システムの変更内容の記録を残すこと。

・ユーザーに影響がある場合は、必要な情報を事前に周知すること。

・システム変更は、サービスへの影響がないことを確認した上で行うこと。

3.3.7.

推奨

システム構成要素の脆弱性情報について、構成要素ごとに次の項目を定めること

・収集先

・収集タイミング

・収集方法

「セキュリティ品質基準」 2.構成要素の脆弱性に対する対策 2-2.システム基盤層の脆弱性対策

補足

・上記のような項目を定めないと、本来収集すべき脆弱性情報(OS、ソフトウェア等)に漏れが生じる可能性が高まる。

・収集先の例：

－製品ベンダのサポート

－Security News Flash （G 外秘）

－JVN, JVN iPedia

・収集方法は、運用体制も含めて実現可能な方法を定めること。

3.3.8.

推奨

業務上必要なソフトウェアのサポート期間を把握し、サポート期限が切れないよう管理ルールを定めること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・内部ユーザーが利用するソフトウェアを含めて管理ルールを定めること。

・定期的に棚卸しを行うこと。
・業務上十分なサポート期間のあるソフトウェアを使用すること。

3.3.9.

推奨

開発生産物は、必要に応じて変更管理手続きに従い変更すること

「情報セキュリティポリシー(規程)」 第5章 プロジェクトのセキュリティ管理 第1節 プロジェクトにおける情報管理

補足
・なし

3.4. ネットワーク管理

3.4.1.

強く推奨

最新のネットワーク構成を把握すること

「社内ネットワークの構築運用管理に関する実施方法」ネットワークの運用 ネットワークの構成管理

補足
・定期的に棚卸しを行うこと。
・不要な機器やソフトウェアを速やかに撤去、又は削除の上、構成情報を最新化すること。
・人手による運用だけではソフトウェアの最新バージョンやパッチの適用管理の徹底が難しい場合に、バージョン管理ソリューションを導入すること。
バージョン管理ソリューションの例：NOSiDE Inventory Sub System （検疫 NW・PC セキュリティ管理・PC 資産管理）

3.4.2.

推奨

開発 LAN で使用する IP アドレスは、認められた範囲のものを使用すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 IP アドレス

補足

・なし

3.4.3.

推奨

IP アドレスを付与する場合は、その必要性を確認し、ネットワーク責任者の承認を得ること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの運用 IP アドレスの付与

補足

・なし

3.4.4.

推奨

リモートアクセス環境の利用資格は、リモートアクセス先のネットワーク利用資格に準拠すること

「社内ネットワークの構築運用管理に関する実施方法」ネットワークの構築 リモートアクセス環境のセキュリティ要件

補足

・なし

3.5. 監視

3.5.1.

必須

不正アクセスの有無を定期的に監視すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 外部接続環境のセキュリティ要件

補足

・認証失敗の急激な増加等から不正なログイン試行を検知できること。

※NTT 持株からの監視強化指示に対応した内容。詳細はセキュリティ品質基準（本編）参照。

・必要に応じて、ツールによる自動監視や外部サービスの利用を検討すること。

・ログローテーションによる確認漏れが生じないよう考慮すること。

3.5.2.

推奨

情報システムの導入後は、利用状況を監視し、問題が発生又は予想される場合は、社内ネットワークを統括する組織に報告すること

「情報システム共通の構築運用管理に関する実施方法」 システム共通部（利用編） 情報システム管理者の留意事項

補足

・なし

3.6. 監査

3.6.1.

必須

システムの構成要素において、次のログを取得すること

・サービスログ

・システムログ

・NW 機器のログ

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-4.ログ管理

補足

・サービスログの例：
- Web サーバのサービスログ
- AP サーバのサービスログ
- メールサーバのサービスログ
- DNS サーバのサービスログ
- 業務アプリケーションにおける認証ログ
- 業務アプリケーションにおける重要な操作ログ
- 不正プログラム対策ソフトの検知ログ
- バックアップのログ
- 認証サーバのログ
- 端末のイベントログ
- Proxy サーバのログ
- URL フィルタリングのログ

・システムログの例：
- OS の認証ログ
- OS のアクセスログ

・NW 機器のログの例：
- ファイアウォールのドロップログ（inbound/outbound）

－IDS/IPS の検知ログ

・システム外との通信や操作に関するログだけではなく、システムの運用管理に使用する端末との通信や操作に関するログも含めること。

・攻撃により異常な量のログが発生した場合も想定し、ログを格納するストレージには十分な空き容量を確保の上、容量監視をすることが望ましい。

3.6.2.

必須

取得ログには、次の項目を記録すること

・日付・時刻

・アクセス主体識別情報

・操作内容

・操作の結果

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-4.ログ管理

補足

・取得ログでは、「いつ、誰（何）が、どこからどこに対して、何を行って、その結果どうなったのか」をトレースできること。

・標的型攻撃対策として、特に以下のログ項目を取得すること。

－メールサーバで取得するログに含める項目：

－受信日時、件名、送信元メールアドレス、送信先メールアドレス、

－添付ファイル名、受信バイト数、ステータス

－Proxy サーバで取得するログに含める項目：

－インターネット上のサイトへのアクセス日時、アクセスしたサイトの URL、

－リクエストの HTTP メソッド、送信元 IP アドレス、

－アクセスした利用者の識別情報、レスポンスステータス（認証結果）、

－UserAgent、受信バイト数、Referer

－DNS キャッシュサーバのログに含める項目：

－内部の端末から DNS キャッシュサーバへの名前解決要求

－問合せ日時、問合せ元 IP アドレス

・Active Directory の場合、ドメインコントローラの監査設定を有効にし、認証の成功および失敗の監査の両方を行うこと。さらに、ドメインに参加する各 Windows サーバでも、同様の設定を行うこと。

3.6.3.

必須

定期的にセキュリティ状態を監査すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 外部接続環境のセキュリティ要件

補足

・認証失敗の急激な増加等から不正なログイン試行を確認できること。

※NTT 持株からの監視強化指示に対応した内容。詳細はセキュリティ品質基準（本編）参照。

・ログローテーションによる確認漏れが生じないよう考慮すること。

3.6.4.

強く推奨

ログを取得しているすべての構成要素は、単一の時計に同期すること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-4.ログ管理

補足

・システム内の取得ログ相互で時刻がずれているとインシデント調査が困難になる。

3.6.5.

強く推奨

ログ溢れにより取得ログが失われることを防ぐため、ログローテーションすること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-4.ログ管理

補足

・大量ログの発生によってディスク容量が圧迫されないよう、保管するログレベル等を考慮の上、ログ設計および容量設計を実施すること。

・短時間でログが上書きされないようなローテーション方法とすることが望ましい。（例：ログファイル名に"yyyymmddhhmm"を付与するなど）

3.6.6.

推奨

端末ではイベントログを取得すること

「セキュリティ品質基準」 4.システムの管理面での対策

補足

・Windows®クライアントのイベントログを想定している。すべての Windows®クライアントでイベントログを取得すること。

・イベントログのサイズが設定値上限に達したら別ファイルに保存する等により、あらかじめ定めた期間はログが消えない設定をすること。

3.6.7.

推奨

取得ログは一定期間保管すること

「セキュリティ品質基準」 1.基本的なセキュリティ機能 1-4.ログ管理

補足

・インシデント発覚後に、過去に遡ってログ調査を実施する必要があるため。

・重要資産を保有するシステムでは、取得ログは 2 年以上保管すること。

・重要資産を保有しない場合でも、取得ログは 1 年以上保管すること。

3.7. 共用サービスの利用

3.7.1.

必須

・ファイルサーバアカウントは必要最小限の利用者に付与すること

・ファイルサーバアカウントは一人ひとりに付与し、共用しないこと

「共有ファイルシステムの構築／運用管理に関する実施方法」 運用 アカウントの管理

補足

・アクセス制御に関しては 2.3.1 の補足を参照。

3.7.2.

推奨

・ファイルサーバの情報システム種別を決定すること

・必要に応じて緊急時の対応計画を立案すること

「共有ファイルシステムの構築／運用管理に関する実施方法」 システム構築 システム種別の決定

補足

・なし

3.7.3.

推奨

・ファイルサーバは共用かつ専用の機器を使用すること

・ファイルサーバの OS 及びソフトウェアはセキュリティを確保できるものを使用すること

「共有ファイルシステムの構築／運用管理に関する実施方法」 システム構築 ファイルサーバの要件

補足

・ファイルサーバは極力組織、担当で共同利用するための専用機器を用意すること。

3.8. 緊急時の対応

3.8.1.

推奨

緊急時に即座に対処が実施できる運用体制を構築すること

「社内ネットワークの構築運用管理に関する実施方法」 ネットワークの構築 外部接続環境のセキュリティ要件

補足

・なし

3.9. サービスの継続

3.9.1.

必須

保管される情報の重要性に応じたバックアップ計画を立て、実施し、回復手順を確立すること

「情報システム共通の構築運用管理に関する実施方法」システム共通部（運用編）システム管理（Ⅲ）データの保護

補足

・不正アクセスや災害等により、データが失われることを防ぐための対策。特に、取得ログはインシデント発生時の原因調査のために必要となるため、失われないようにすること。また、そのデータが失われることにより、その後の業務の継続に多大な影響を及ぼすような重要な業務データについても、失われないようにすること。

・バックアップの際に、取得ログと業務データを同じ場所にバックアップすると、業務データに不正アクセスしようとする攻撃者（内部犯行）が取得ログも改ざんできる可能性が高くなるため、取得ログと業務データは別々にバックアップすること。なお、別々にバックアップとは、必ずしもバックアップ媒体を別にすることだけを意図しているものではなく、格納場所が論理的に分かれていればよい。

・メール添付ファイルを開くことが避けられない業務等、ランサムウェアによる攻撃リスクが高い場合、バックアップデータはオフラインで保存することが望ましい。

・バックアップ対象の取得ログは、書き込み中の取得ログではなく、他のサーバに転送した取得ログ等、静的なファイルを対象としている。

・取得したバックアップから正しくリストアできることを確認しておくこと。

3.9.2.

推奨

情報システムのサービス中断の影響が大きい場合は、事前に情報システム責任者に連絡するとともに、利用者に周知を行うこと

「情報システム共通の構築運用管理に関する実施方法」システム共通部（運用編）システム停止

補足

・なし

第 4 章　引用元ドキュメント

引用元ドキュメントに関しては以下に記載された URL から確認することができます。

https://security.groupwide.net/isec/guideline/saisoku_etc_new