intloop（イントループ） × TECH STOCK

ネットワーク接続時における情報セキュリティ対策の最適化

概要

ITの普及に伴い、業務を遂行するために、あらゆるものがネットワークを経由して、接続されることが必要不可欠となりました。
そこで、

- ネットワーク接続時における情報セキュリティ対策とは？
- 対策が間違っていたら？
- 対策方針を検討するときの考慮するポイントは？

を具体例を用いてご紹介します。

現場の対策方針に疑問を持っている方、改めて対策方針を見直そうと考えている方、
是非ご一読ください。

目次

1. ネットワークセキュリティ対策とは

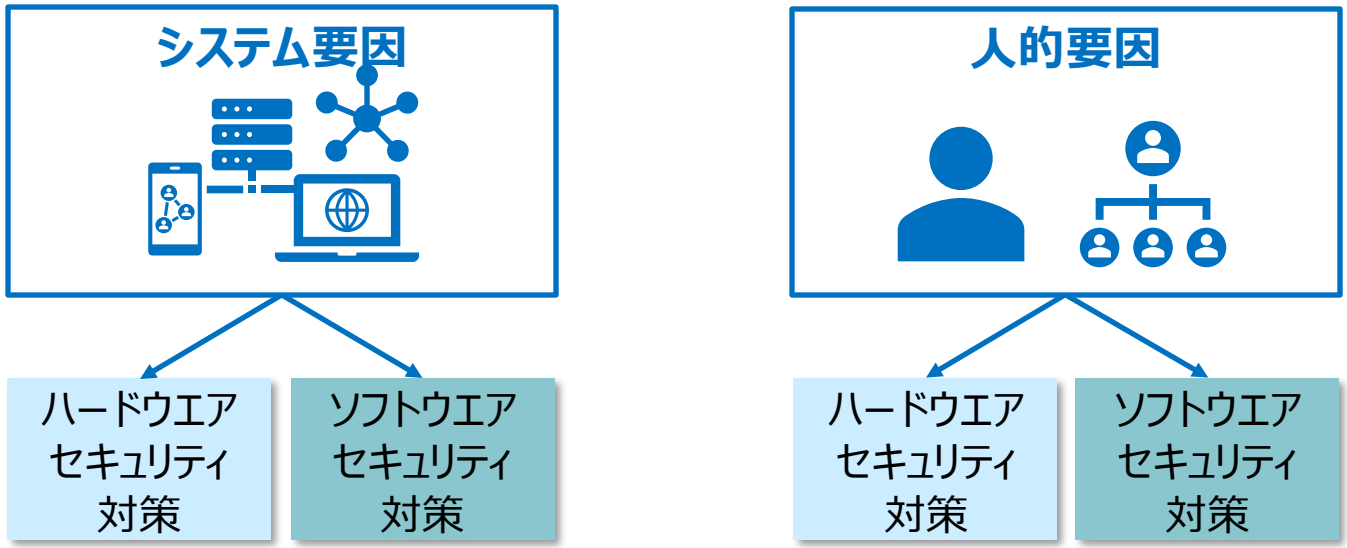
2. ネットワークセキュリティ対策で考慮するポイント【技術面】

3. ネットワークセキュリティ対策で考慮するポイント【運用面】

4. まとめ

ネットワークセキュリティ対策とは～情報セキュリティー対策～

情報セキュリティ対策とは、企業や個人が保有する情報資産を、様々な脅威から守り、
機密性・安全性・可用性を確保して運用するための施策のことを指します



情報資産を守るための情報セキュリティ対策には、システム要因（物理・技術）、人的要因（人・組織）と要因別にハードウェアセキュリティ対策、ソフトウェアセキュリティ対策などの各対策に分類できます。

出展元：総務省 「国民のための情報セキュリティサイト」URL）https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
日本ネットワークセキュリティ協会「情報セキュリティの基礎」 URL） https://www.jnsa.org/ikusei/01/02-05.html

ネットワークセキュリティ対策とは～情報資産を守る現代の対策～

情報セキュリティ対策の対象となっている情報資産には、企業や個人に分けて以下のものが挙げられます。

		企業	個人
情報資産	重要情報	顧客情報、財務情報、購買情報など	住所、氏名、カード番号など
	データ	重要情報を記載したファイル、電子メール	重要情報を記載したファイル、電子メール
	記憶媒体	データが保存・記載されているコンピュータ、USBなど	データが保存・記載されているコンピュータやUSB

本文書は、業務を遂行するためにネットワーク接続が必要になった時代に欠かせないネットワークセキュリティに着目しました。

出展元：総務省 「国民のための情報セキュリティサイト」URL）https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
日本ネットワークセキュリティ協会「情報セキュリティの基礎」 URL） https://www.jnsa.org/ikusei/01/02-05.html

ネットワークセキュリティ対策とは～脅威の例（外部要因・内部要因）～

インターネット対応端末（PCやスマートフォン端末・タブレット端末）のネットワーク接続に伴い、
外部要因によるセキュリティ被害は年々増えています。

総務省が発表した「企業の情報通信ネットワークにおける被害状況・被害内容（令和元年版）」
によりますと、被害内容の上位3位は以下の通りでした。

外部要因

1. ウィルスを発見またはウィルスに感染
2. スパムメールの中継利用・踏み台
3. システムへの不正アクセス

**外部要因に向けて対策していた場合でも
内部要因（人的要因）により、
情報資産の漏洩やセキュリティ被害の
加害者になる可能性もあります。**

内部要因

1. ウイルス対策ソフトの未活用および未更新
2. ファイル共有ソフトの使用
3. 社外（喫茶店など）にて、端末放置して離席

内部要因における対策も重要となります。

出展元：総務省 「情報通信統計データベース」「国民のための情報セキュリティサイト」
URL）https://www.soumu.go.jp/johotsusintokei/field/sonohoka01.html
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

ネットワークセキュリティ対策とは～セキュリティ事項の例　３選～

セキュリティ対策を誤った場合、下記例のようなセキュリティ事故が発生する可能性が高まります。
外部要因は技術面、内部要因は運用面にてセキュリティ対策を考慮することが防止策となります。

1 ネットワークに接続するIoT機器やシステムによるサイバー攻撃やシステム障害の発生

原因	外部要因	内部要因
ネットワークに接続するリスクを認識していなかった	✓	
IoT機器特有のリスクを認識していなかった	✓	
システムに侵入された場合を想定した対策を行えていなかった	✓	

2 標的型攻撃により、1台のコンピュータがウイルス感染し、重要情報の漏洩

原因	外部要因	内部要因
被害を最小限にする対策が行えてなかった	✓	
IoT機器特有のリスクを認識していなかった		✓
システムに侵入された場合を想定した対策を行えていなかった		✓

3 システムの脆弱性を狙い、システム妨害行為（例：zoom爆弾）

原因	外部要因	内部要因
脆弱性を認識していなかった	✓	
ウイルス対策ソフトのウイルス検知用データの更新を怠った		✓

出展元：総務省「国民のための情報セキュリティサイト」　「IOTセキュリティガイドライン」
URL）https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
https://www.soumu.go.jp/main_content/000428393.pdf

1. ネットワークセキュリティ対策とは

2. ネットワークセキュリティ対策で考慮するポイント【技術面】

3. ネットワークセキュリティ対策で考慮するポイント【運用面】

4. まとめ

ネットワークセキュリティ対策で考慮するポイント【技術面】

総務省より提供されている、セキュリティガイドラインに記載されている対策方法の中から、
3つご紹介します。

リスクを認識する

社内環境や使用しているシステム特有のリスクが存在するため、全てのリスクを認識したうえで対策を検討することが大切です。
また、対策実施後に社内環境やシステムに変化があった場合はセキュリティ対策が合っているか、再検討することも必要です。

守れる設計を行う

全ての情報資産を守れることが理想ですが、現実的ではありません。
全ての情報資産の中から、守るべき対象を明確にし、明確にした対象を守れる設計を行うことが大切です。

出口対策を行う

対策によって、セキュリティ事故が起こらないことが第一ですが
万が一の場合に、システム障害や情報漏洩が起こらないように
出口対策(データの暗号化等)も重要な対策のひとつです。

出展元：総務省「国民のための情報セキュリティサイト」　「IOTセキュリティガイドライン」
URL）https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
https://www.soumu.go.jp/main_content/000428393.pdf

1. ネットワークセキュリティ対策とは

2. ネットワークセキュリティ対策で考慮するポイント【技術面】

3. ネットワークセキュリティ対策で考慮するポイント【運用面】

4. まとめ

ネットワークセキュリティ対策で考慮するポイント【運用面】

総務省より提供されている、セキュリティガイドラインに記載されている対策方法の中から、
3つご紹介します。

実現可能な内容とする

万全なセキュリティ対策でも社内状況（運営体制や維持体制）に合っていなければ、情報セキュリティ対策は行えず、リスクにつながります。
社内状況を考慮し、実現可能な内容を考えることが大切です。

対象者の範囲を明確にする

情報資産を扱うシステムが誰にでも使用・閲覧できた場合、ネットワークセキュリティ対策は脆くなります。
そのため、対象者の範囲を明確にし、使用・閲覧の権限を各々設定することが大切です。

セキュリティ教育を行う

システムや社内状況に合わせたネットワークセキュリティ対策を行っても、情報を扱う方が運用ルールを守らなければ、無意味になります。業務等で使用するシステムでのリスク・対策方法を説明し、内部不正やミスをなくすため、セキュリティ教育は必要不可欠です。

出展元：総務省「国民のための情報セキュリティサイト」　「IOTセキュリティガイドライン」
URL）https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
https://www.soumu.go.jp/main_content/000428393.pdf

1. ネットワークセキュリティ対策とは

2. セキュリティ対策の失敗例

3. ネットワークセキュリティ対策で考慮するポイント【技術面】

4. ネットワークセキュリティ対策で考慮するポイント【運用面】

5. まとめ

まとめ

ネットワークセキュリティー対策についてのポイントを挙げておきます

1 対策を検討する側、業務を実施する側双方の意識づけが重要

セキュリティ対策を考える側は「常にアップデートされる状況（システム特有のリスク、社内体制、守るべき情報資産）」、セキュリティ対策に基づき業務を行う側は、「自分の考え方・行動ひとつでセキュリティ事故が発生すること」を認識することが大切です。

2 最大限の対策をおこなっていても、事故発生の可能性はゼロではない

最大限のセキュリティ対策を行っていても、セキュリティ事故が起こる可能性があります。
セキュリティ事故が起こった場合には、システム要因・人的要因を追求したうえで、
改めてセキュリティ対策案を検討する必要があります。

3 現在の状況に適した対策にアップデートすることが重要

今一度、企業のセキュリティ対策・個人のセキュリティ対策への考え方を見直し、
現在の状況に適したネットワークセキュリティ対策にアップデートをすることをオススメいたします。

INTLOOPについて

さまざまな経営課題の解決を支援するコンサルティング事業を主軸に、テクノロジーを駆使しビジネスモデルの変革を目指すデジタルトランスフォーメーション事業、 システムの開発・導入を支援するテクノロジーソリューション事業、専門性の高い人材をご紹介する人材ソリューション事業の4事業を柱に事業を展開。

常にお客様の視点に立つことを第一義に考え、お客様の課題に対して最適なソリューションを提供し続けています。

お問合せ

下記フォームよりお問合せください。

https://www.intloop.com/contact/general/

記載の企業ロゴデザインについて

記載している企業のロゴ、商標は企業が提示しているガイドラインを確認したうえで記載しています。
デザイン、商標についての著作権は、それぞれの企業に帰属しています。

免責事項

この文書に記載されている情報は一般的なものであり、特定の個人や組織に対するアドバイスを提供するものではありません。掲載情報の正確さについてできる限りの努力をしていますが、その正確性や適切性を保証するものではありません。
何らかの行動をとられる場合は、本資料の情報のみを根拠とせず、専門家による適切な分析・アドバイスをもとにご判断ください。当資料を用いて行う一切の行為、被った損害・損失に対しては当社は一切の責任を負いかねます。予めご了承ください。
当資料の著作権は当社にあります。当資料の転載、流用、転売など、ダウンロードされたご本人様以外のご利用は固くお断りさせていただきます。