情報セキュリティとその対策

升井　洋志
北見工業大学 情報処理センター
センター長・教授

情報セキュリティの基礎

最近の事例より

沖縄の最近の事例

那覇市立図書館の図書館システムのランサムウェア攻撃

2022年10月、那覇市立図書館の図書館システムがランサムウエア攻撃を受けた。
バックアップを含むデータが暗号化され、貸し出しサービスを一時停止した。
侵入経路はシステムを遠隔からメンテナンスするためのVPN装置とみられる。
身代金を支払うことなく、システムの代替となる手段を講じながら開館を続けた。
攻撃の3カ月後である2023年1月から、再構築したシステムを順次稼働させた。

日経クロステック／日経コンピュータ
https://xtech.nikkei.com/atcl/nxt/column/18/01157/040500083

沖縄の最近の事例

那覇市立図書館の図書館システムのランサムウェア攻撃

1. 発生日時, 場所（対象）, 状況
2. 対象となる情報資産
3. 被害状況・影響範囲
4. 侵入経路
5. 復旧への対応
6. 再発防止

1. 発生日時, 場所（対象）, 状況

日時: 2022年10月13日発生

場所（対象）：那覇市図書館・図書館システム

状況: 図書館システムへのランサムウェア攻撃

2. 対象となる情報資産

・那覇市図書館システムの蔵書データ

・図書館システムのアプリケーションファイル

・ログ等のシステムファイル

3. 被害状況・影響範囲

・システム本体およびバックアップが暗号化

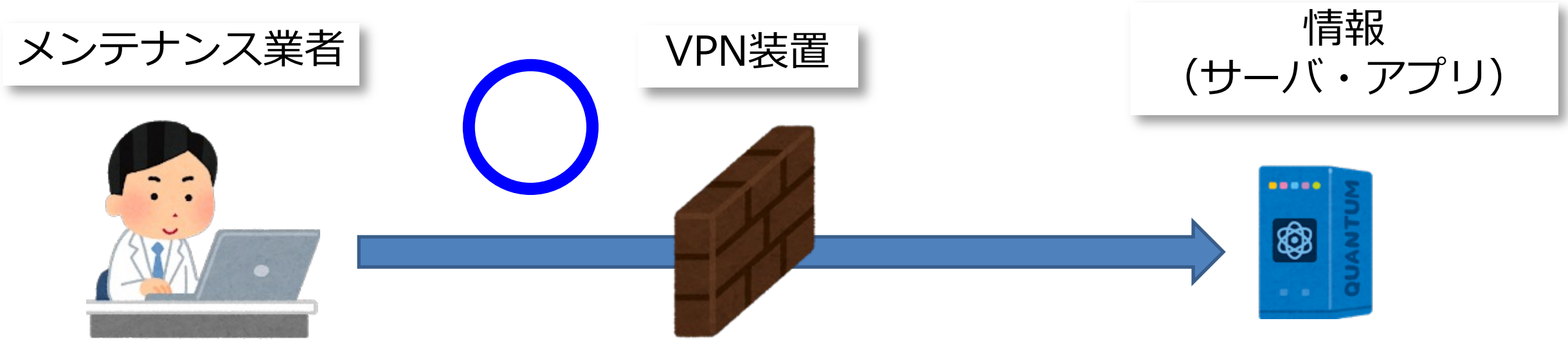
・貸出作業不能のためサービスを一時停止

・その後手動（Excelファイル）でサービス再開

4. 侵入経路

・リモートメンテナンス用のVPN装置から侵入した（と見られる）

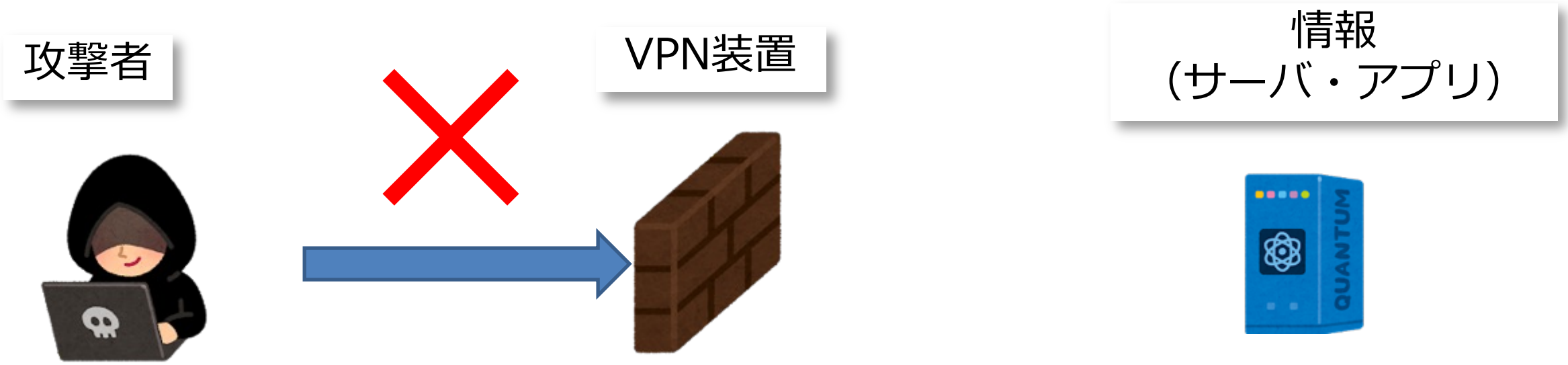
「安全なはず」のVPN装置から侵入



4. 侵入経路

・リモートメンテナンス用のVPN装置から侵入した（と見られる）

「安全なはず」のVPN装置から侵入



5. 復旧への対応

ハンディスキャナでの貸出作業開始（翌日から一旦中止）

Excelの共有による貸出作業復旧

利用者の再登録

Excelはクラウド上で共有管理

クラウド上のExcelと各図書館のバーコードリーダを連携

本格的な復旧は3ヶ月後

6. 再発防止

VPN装置のこまめなアップデート

（できれば以下も）

接続元の制限

データの分散バックアップ

ランサムウェア対応のストレージ導入

情報セキュリティとインシデント対応

1. 発生日時, 場所（対象）, 状況	記録
2. 対象となる情報資産	情報資産の分類（格付け）
3. 被害状況・影響範囲	情報資産の分類（格付け）
4. 侵入経路	セキュリティ対策の分類
5. 復旧への対応	インシデント発生時の運用
6. 再発防止	対策の具体化

類似の事例

日野市図書館システムのランサムウェア攻撃

令和4年12月17日に、図書館の一部の業務用ファイルサーバ等がコンピュータウィルスのランサムウェアに感染したことが判明いたしました。現在、原因究明と被害範囲の特定を進めています。貸出システム等大部分のシステムは被害を受けていないため、図書館は通常通り開館しています。

ファイルサーバ内に格納されているデータが暗号化されて開けない状態。その中に個人情報（図書館主催のイベントの参加者、障害者サービスの利用者・ボランティアの名簿等）があることを確認しています。なお、現時点で情報の流出は確認されていません。

日野市HPより
https://www.city.hino.lg.jp/press/1022253/1023008.html

類似の事例

埼玉大学業務システムのランサムウエア被害

埼玉大学は業務利用のシステムがランサムウエアに感染し、データの一部が改変されたと公表した。

　不正アクセス被害に遭ったのはNAS（ネットワーク接続型ストレージ）。2022年6月7日午前8時ごろに実施したネットワークアクセス制限の設定変更に不備があり、外部からNASにアクセスできるようになった。同日正午には攻撃者から複数回のログオンが試行され、2台のNASのパスワードが破られた。さらに、そのNASを踏み台に別の4台のNASが不正アクセスを受け、ランサムウエアによってデータの一部が改変されたという。

日経クロステック／日経コンピュータ
https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/031800050/031600049

類似の事例

島根大学附属図書館のWebサーバに不正アクセス

島根大学によると、同学附属図書館のホームページ等を公開しているWebサーバにおいて，利用者向けのアンケート調査や主催するイベントへの申込みを受け付けるために公開していたアンケート管理システムのサイバーセキュリティ対策に脆弱性が見つかり、アンケート調査やイベントへの参加申込みのために入力された個人情報が外部から閲覧可能な状態になっていたことが分かったとのことです。個人情報漏えいの可能性がある利用者には，郵送やメール等で個別にご連絡と，お詫びとご報告を実施するとしています。

サイバーセキュリティソリューションズ
https://www.cybersecurity.co.jp/incident/島根大学%E3%80%80附属図書館のwebサーバに不正アクセス/

類似の事例

大英図書館へのサイバー攻撃

Yahoo Newsによると、大英図書館は利用者データがサイバー攻撃でハッキングされ、ダークウェブで売りに出されていることを確認した。同図書館は、他の場所で同じパスワードを使用している利用者に対し、パスワードを変更するよう勧告している。この攻撃は10月31日に発生し、図書館のウェブサイト、オンラインシステム、一部のオンサイトサービスに影響が続いている。Rhysidaランサムウェアグループはこの攻撃の責任を主張し、盗まれたデータをオークションにかける計画を発表している。

Coinilve
https://www.coinlive.com/ja/news-flash/342874

インシデント発生状況一覧サイト

サイバーセキュリティ.com 「個人情報漏洩事件・被害事例一覧」

https://cybersecurity-jp.com/leakage-of-personal-information

2024年

日付	法人・団体名	件数・人数	漏洩原因	漏洩内容・詳細・二次被害（悪用）など
2024/2/28	株式会社企業農業研究所（なかほら牧場）	1万4,933件	不正アクセス	2024年2月28日、同社が運営していたオンラインショップ「なかほら牧場オンラインストア」が外部からのサイバー攻撃を受け、過去オンラインストアで情報を入力したユーザーのクレジットカード情報5,069件やこれを含む個人情報1万4,933件が流出した可能性があると明らかにした。
2024/2/26	東京外国語大学	約2万6,000件	不正アクセス	2024年2月26日、同大メールシステム利用者1名のアカウントが不正アクセスされ、合計約2万6,000件の不審メールを送信していたと明らかにした。
2024/2/21	株式会社アテクト	2,055件	誤送信	2024年2月21日、顧客向けに発した電子メールについて誤送信が発生し、メールアドレス2,055件が外部流出したと明らかにした。
				2024年2月21日、職員が使用する業

3つのセキュリティ

1. 物理的セキュリティ

盗難、不法侵入、破壊

2. 技術的セキュリティ

ハッキング、脆弱性攻撃、DoS攻撃

3. 人的セキュリティ

ウィルス感染、パスワード漏洩、設定ミス

1. 不正プログラム対策

「不正プログラム」

通常の動作・期待される機能でなく、悪意を持った動作をするプログラム

「悪意のある」という意味の”malicious”という単語から、
一般には「マルウェア(malware)」と呼ばれる

昔は「コンピュータウィルス」または単に「ウィルス」と呼ばれていたが、現在ではスパイウェアやランサムウェア等、いろいろなものが出てきたので「マルウェア」と読んでいる。

不正プログラムの種類

・ウィルス：通常のソフトウェアに「感染」する形で侵入するもの

・ワーム: 「感染」を必要とせず、単体で動作するもの

・トロイの木馬:有益なソフトに見せかけて侵入するもの

・スパイウェア: 侵入したコンピュータの情報を盗むもの

・アドウェア: 広告を勝手に表示するもの

・ルートキット: コンピュータの管理者権限を利用して改竄等を行うもの

・ランサムウェア: コンピュータ内の情報を「人質」にして金銭を要求するもの

・ボット: 外部から標的を攻撃するもの

不正プログラムの目的

昔はどちらかと言えばコンピュータ内の情報を破壊するものが主流

ウィルス

ハードディスクの初期化
ソフトウェアの改竄

「情報」はお金になる

コンピュータ内の情報を盗む、情報をお金にする

スパイウェア
トロイの木馬

ランサムウェア

代表的なランサムウェア

“WannaCry”（ワナクライ）　“泣きたい”

2017年ごろに世界中で猛威を振るったランサムウェア

コンピュータ上のファイルを勝手に暗号化し、
身代金としてビットコインを要求した

（現金だと「足がつく」ので）

世界中の企業・個人が被害にあった

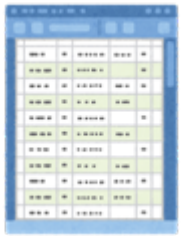
身代金要求の画面

脆弱性と感染源

OSやソフトウェアの不備をついて、感染を行う

脆弱性

感染ルートは多岐にわたる



- メールの添付ファイル
- Excelのマクロ
- USBメモリ
- ブラウザのリンク、ダウンロード
- ネットワークを通じて外部から

脆弱性を排除するには

※原理的には、コンピュータ内の全てのプログラム・ライブラリ等が
　完璧であれば脆弱性は発生しない。

→ もちろん、そんなのは無理な話である

「どのくらい脆弱性があるか」は検疫ソフトウェア等の
脆弱性診断を用いることでわかる

が、一般的にはお高い

アンチウィルスソフト

通常、マルウェア対策にはアンチウィルスソフトを使う

「アンチウィルス」だとウィルスにしか対応してないみたいなので、
最近では「エンドポイントプロテクション（末端保護）」や
「エンドポイントセキュリティ」と呼ぶ

・パターンマッチング

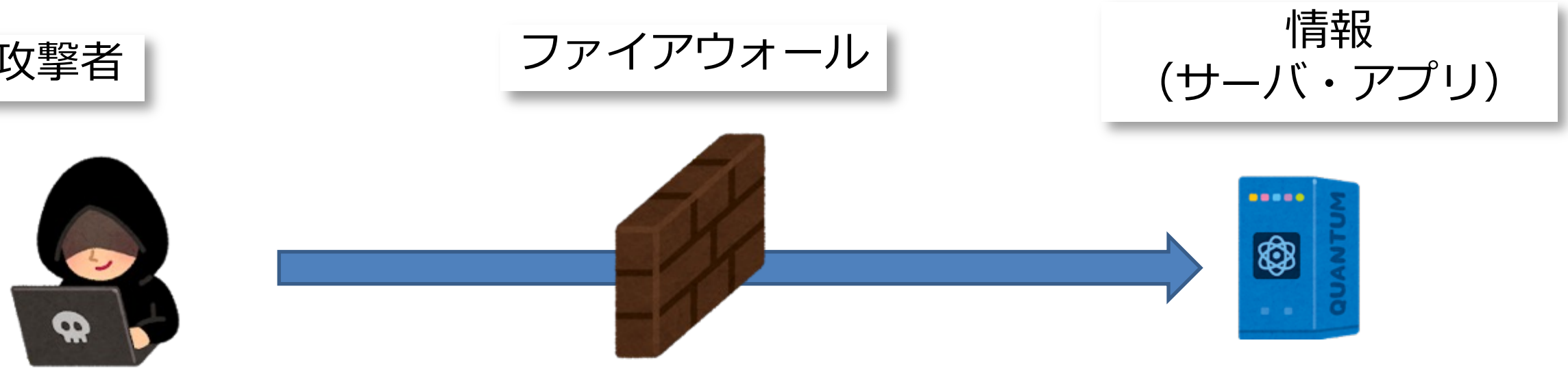
・振る舞い検知

・動作制御

膨大なデータをAI処理することで、より検知精度を上げている

ファイアウォール

特定の通信内容、特定のIPアドレス以外を遮断する



通常はコンピュータ（PC）自体にもファイアウォールが入っている

さまざまな防止策

・不正侵入検知システム（IDS: Intrusion Detection System）

・侵入阻止システム（IPS: Intrusion Prevention System）

・検疫システム

ネットワークに接続された端末が安全かを見張るシステム

・アプリケーションファイアウォール（WAF: Web Application Fiwewall）

Webサーバの脆弱性をカバーするように動作するファイアウォール

防御の限界

永遠のイタチごっこ

攻撃者

対策

情報
（サーバ・アプリ）

別の方法

1. システムの固定化

コンピュータのシステムファイルが変更できないようにする

・再起動時に初期化
・固定イメージから起動し、イメージを書き換えさせない

情報端末室のPCはこの方法

2. システムのバックアップ

改竄された場合に備えてバックアップしておく

3つのセキュリティ

1. 物理的セキュリティ

盗難、不法侵入、破壊

2. 技術的セキュリティ

ハッキング、脆弱性攻撃、DoS攻撃

3. 人的セキュリティ

ウィルス感染、パスワード漏洩、設定ミス

「物理的セキュリティ」

- サーバ、データの物理的な盗難防止
- 電子データ媒体、紙媒体の管理・破棄
- 電源のバックアップ

1. 物理的セキュリティ

「盗難」や「不法侵入」に気をつけましょう

⇒これは、だいたいわかっているつもり、、、

以下の点に注意

- 鞄の中にPCやスマホを入れっぱなして食堂の席取り
- クルマのエンジンをかけっぱなしでコンビニ
- アパートの鍵をかけないで外出

「技術的セキュリティ」

- サーバ、PCのセキュリティ対策
- ネットワークのセキュリティ対策
- 攻撃防御と攻撃検知

脆弱性

- 古いバージョンのOS, アプリケーション
- デフォルト設定のサーバ・ファイアウォール
- 暗号化されていない通信
- アプリケーション、スクリプトのデフォルト設定
- 簡単なパスワード、ブルートフォースアタック非対策

「人的セキュリティ」

- ID/パスワード漏洩対策
- メール添付ファイル対策
- 設定ミスの解消
- 共有ユーザの管理
- ユーザのライフサイクル管理

表 1.3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

IPA: 情報処理推進機構「情報セキュリティ10大脅威 2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html
https://www.ipa.go.jp/files/000088835.pdf

認証：ログインのアクセス制御

ID管理

パスワード管理

認証方式の複雑化（多要素認証）

- 簡単な文字列にしない
- 初期パスワードのままにしない

  「定期的な変更」は必ずしも良い結果になるとは限らない
- 同じパスワードを別サービスで使わない
- 他人に教えない、紙に書いておかない

電子メールのセキュリティ

・メールアドレスの信憑性

なりすましメール（送信者偽装）

・メール送受信時の暗号化

通信経路の暗号化（とくに無線LAN）

メール本体の暗号化（PGP, S-MIME）

・ウィルス対策

ウィルス除去サーバ

エンドポイントセキュリティ（アンチウィルスソフト）

メールアドレスの信憑性

インターネット上でメールを送受信するには
SMTPと言われるプロトコルを用いる。

（SMTP: Simple Mail Transfer Protocol）

これはインターネット黎明期からある仕組みで
「なりすまし防止」や「暗号化」等の直接の実装が無い。

（「古き良き時代」の名残りを使い続けている状態）

なりすまし防止にはメール配送時にDNSで送信メールサーバが
実在するかを確認する仕組み（SPF等）を用いる。

しかし、実在するメールサーバからSPAMメールを送りつけられる
ような場合に対しては無力である。

まとめ

・セキュリティは日々の積み重ね

記録

情報資産の分類（格付け）

セキュリティ対策の分類

インシデント発生時の運用

対策の具体化

・「なにも起こっていない」ということはあり得ない

・何事も疑ってかかるのも一つ

“That's one small step for (a) man, one giant leap for mankind.”
Neil Armstrong, On the surface of the moon, 1969.