問３　継続的インテグレーションサービスのセキュリティに関する次の記述を読んで，設問に答えよ。

N 社は，N サービスという継続的インテグレーションサービスを提供している従業員 400 名の事業者である。N サービスの利用者（以下，N サービス利用者という）は，バージョン管理システム（以下，VCS という）にコミットしたソースコードを自動的にコンパイルするなどの目的で，N サービスを利用する。VCS では，リポジトリという単位でソースコードを管理する。N サービスの機能の概要を表 1 に示す。

表 1　N サービスの機能の概要（抜粋）

機能名	概要
ソースコード取得機能	リポジトリから最新のソースコードを取得する機能である。N サービス利用者は，新たなリポジトリに対して N サービスの利用を開始するときに，そのリポジトリを管理する VCS のホスト名及びリポジトリ固有の認証用 SSH 鍵を登録する。ソースコードの取得は，VCS から新たなソースコードのコミットの通知を HTTPS で受け取ると開始される。
コマンド実行機能	ソースコード取得機能がリポジトリからソースコードを取得した後に，リポジトリのルートディレクトリにある ci.sh という名称のシェルスクリプト（以下，ビルドスクリプトという）を実行する機能である。N サービス利用者は，例えば，コンパイラのコマンドや，指定された Web サーバにコンパイル済みのバイナリコードをアップロードするコマンドを，ビルドスクリプトに記述する。
シークレット機能	ビルドスクリプトを実行するシェルに設定される環境変数を，N サービス利用者が登録する機能である。登録された情報はシークレットと呼ばれる。N サービス利用者は，例えば，指定された Web サーバに接続するために必要な API キーを登録することによって，ビルドスクリプト中に API キーを直接記載しないようにすることができる。

N サービスは C 社のクラウド基盤で稼働している。N サービスの構成要素の概要を表 2 に示す。

表2　Nサービスの構成要素の概要（抜粋）

Nサービスの構成要素	概要
フロントエンド	VCS から新たなソースコードのコミットの通知を受け取るための API を備えた Web サイトである。
ユーザーデータベース	各 N サービス利用者が登録した VCS のホスト名，各リポジトリ固有の認証用 SSH 鍵，及びシークレットを保存する。読み書きはフロントエンドからだけに許可されている。
バックエンド	Linux をインストールしており，ソースコード取得機能及びコマンド実行機能を提供する常駐プログラム（以下，CI デーモンという）が稼働する。インターネットへの通信が可能である。バックエンドは 50 台ある。
仮想ネットワーク	フロントエンド，ユーザーデータベース及びバックエンド 1～50 を互いに接続する。

フロントエンドは，ソースコードのコミットの通知を受け取ると図1の処理を行う。

1. 通知を基にNサービス利用者とリポジトリを特定し，そのNサービス利用者が登録したVCSのホスト名，各リポジトリ固有の認証用 SSH 鍵，及びシークレットをユーザーデータベースから取得する。
2. バックエンドを一つ選択する。
3. 2.で選択したバックエンドのCIデーモンに1.で取得した情報を送信し，処理命令を出す。

図1　フロントエンドが行う処理

CI デーモンは，処理命令を受け取ると，特権を付与せずに新しいコンテナを起動し，当該コンテナ内でソースコード取得機能とコマンド実行機能を順に実行する。

ビルドスクリプトには，利用者が任意のコマンドを記述できるので，不正なコマンドを記述されてしまうおそれがある。さらに，不正なコマンドの処理の中には，①コンテナによる仮想化の脆弱性を悪用しなくても成功してしまうものがある。そこで，バックエンドには管理者権限で稼働する監視ソフトウェア製品 X を導入している。製品 X は，バックエンド上のプロセスを監視し，プロセスが不正な処理を実行していると判断した場合は，当該プロセスを停止させる。

C 社は，C 社のクラウド基盤を管理するための Web サイト（以下，クラウド管理サイトという）も提供している。N 社では，クラウド管理サイト上で，クラウド管理サイトのアカウントの管理，N サービスの構成要素の設定変更，バックエンドへの管理者権限でのアクセス，並びにクラウド管理サイトの認証ログの監視をしている。N 社

では，C 社が提供するスマートフォン用アプリケーションソフトウェア（以下，スマートフォン用アプリケーションソフトウェアをアプリという）に表示される，時刻を用いたワンタイムパスワード（TOTP）を，クラウド管理サイトへのログイン時に入力するように設定している。

N 社では，オペレーション部がクラウド管理サイト上で N サービスの構成要素の設定及び管理を担当し，セキュリティ部がクラウド管理サイトの認証ログの監視を担当している。

〔N 社のインシデントの発生と対応〕

1 月 4 日 11 時，クラウド管理サイトの認証ログを監視していたセキュリティ部の H さんは，同日 10 時にオペレーション部の U さんのアカウントで国外の IP アドレスからクラウド管理サイトにログインがあったことに気付いた。

H さんが U さんにヒアリングしたところ，U さんは社内で同日 10 時にログインを試み，一度失敗したとのことであった。U さんは，同日 10 時前に電子メール（以下，メールという）を受け取っていた。メールにはクラウド管理サイトからの通知だと書かれていた。U さんはメール中の URL を開き，クラウド管理サイトだと思ってログインを試みていた。H さんがそのメールを確認したところ，URL 中のドメイン名はクラウド管理サイトのドメイン名とは異なっており，U さんがログインを試みたのは偽サイトだった。H さんは，同日 10 時の国外 IP アドレスからのログインは②攻撃者による不正ログインだったと判断した。

H さんは，初動対応としてクラウド管理サイトの U さんのアカウントを一時停止した後，調査を開始した。U さんのアカウントの権限を確認したところ，フロントエンド及びバックエンドの管理者権限があったが，それ以外の権限はなかった。

まずフロントエンドを確認すると，Web サイトのドキュメントルートに“/.well-known/pki-validation/”ディレクトリが作成され，英数字が羅列された内容のファイルが作成されていた。そこで，③RFC 9162 に規定された証明書発行ログ中の N サービスのドメインのサーバ証明書を検索したところ，正規のもののほかに，N 社では利用実績のない認証局 R が発行したものを発見した。

バックエンドのうち 1 台では，管理者権限をもつ不審なプロセス（以下，プロセス Y という）が稼働していた（以下，プロセス Y が稼働していたバックエンドを被害バ

ックエンドという)。被害バックエンドのその時点のネットワーク通信状況を確認すると，プロセスYは特定のCDN事業者のIPアドレスに，HTTPSで多量のデータを送信していた。TLSのServer Name Indication (SNI) には，著名なOSS配布サイトのドメイン名が指定されており，製品Xでは，安全な通信だと判断されていた。

詳しく調査するために，TLS通信ライブラリの機能を用いて，それ以降に発生するプロセスYのTLS通信を復号したところ，HTTP Hostヘッダーでは別のドメイン名が指定されていた。このドメイン名は，製品Xの脅威データベースに登録された要注意ドメインであった。プロセスYは，④監視ソフトウェアに検知されないようにSNIを偽装していたと考えられた。TLS通信の内容には被害バックエンド上のソースコードが含まれていた。Hさんはクラウド管理サイトを操作して被害バックエンドを一時停止した。Hさんは，⑤プロセスYがシークレットを取得したおそれがあると考えた。

Hさんの調査結果を受けて，N社は同日，次を決定した。

・不正アクセスの概要とNサービスの一時停止をN社のWebサイトで公表する。
・被害バックエンドでソースコード取得機能又はコマンド実行機能を利用した顧客に対して，ソースコード及びシークレットが第三者に漏えいしたおそれがあると通知する。

Hさんは図2に示す事後処理と対策を行うことにした。

1. フロントエンド及び全てのバックエンドを再構築する。
2. 認証局Rに対し，Nサービスのドメインのサーバ証明書が勝手に発行されていることを伝え，その失効を申請する。
3. 偽サイトでログインを試みてしまっても，クラウド管理サイトに不正ログインされることのないよう，クラウド管理サイトにログインする際の認証を⑥WebAuthn (Web Authentication) を用いた認証に切り替える。
4. Nサービスのドメインのサーバ証明書を発行できる認証局を限定するために，Nサービスのドメインの権威DNSサーバに，Nサービスのドメイン名に対応する [a] レコードを設定する。

図2　事後処理と対策（抜粋）

〔N社の顧客での対応〕

Nサービスの顧客企業の一つに，従業員1,000名の資金決済事業者であるP社がある。P社は，決済用のアプリ（以下，Pアプリという）を提供しており，スマートフォンOS開発元のJ社が運営するアプリ配信サイトであるJストアを通じて，Pアプリの利用者（以下，Pアプリ利用者という）に配布している。P社はNサービスを，最新版ソースコードのコンパイル及びJストアへのコンパイル済みアプリのアップロードのために利用している。P社には開発部及び運用部がある。

Jストアへのアプリのアップロードは，J社の契約者を特定するための認証用APIキーをHTTPヘッダーに付加し，JストアのREST APIを呼び出して行う。認証用APIキーはJ社が発行し，契約者だけがJ社のWebサイトから取得及び削除できる。また，Jストアは，アップロードされる全てのアプリについて，J社が運営する認証局からのコードサイニング証明書の取得と，対応する署名鍵によるコード署名の付与を求めている。Jストアのアプリを実行するスマートフォンOSは，各アプリを起動する前にコード署名の有効性を検証しており，検証に失敗したらアプリを起動しないようにしている。

P社は，Nサービスのソースコード取得機能に，Pアプリのソースコードを保存しているVCSのホスト名とリポジトリの認証用SSH鍵を登録している。Nサービスのシークレット機能には，表3に示す情報を登録している。

表3　P社がNサービスのシークレット機能に登録している情報

シークレット名	値の説明
APP_SIGN_KEY	コード署名の付与に利用する署名鍵とコードサイニング証明書
STORE_API_KEY	Jストアにアプリをアップロードするための認証用APIキー

Pアプリのビルドスクリプトには，図3に示すコマンドが記述されている。

1. コンパイラのコマンド
2. 生成されたバイナリコードにAPP_SIGN_KEYを用いてコード署名を付与するコマンド
3. STORE_API_KEYを用いて，署名済みのバイナリコードをJストアにアップロードするコマンド

図3　ビルドスクリプトに記述されているコマンド

1月4日，P社運用部のKさんがN社からの通知を受信した。それによると，ソースコード及びシークレットが漏えいしたおそれがあるとのことだった。Kさんは，⑦Pアプリ利用者に被害が及ぶ攻撃が行われることを予想し，すぐに二つの対応を開始した。

Kさんは，一つ目の対応として，⑧漏えいしたおそれがあるので，STORE_API_KEYとして登録されていた認証用APIキーに必要な対応を行った。また，二つ目の対応として，APP_SIGN_KEYとして登録されていたコードサイニング証明書について認証局に失効を申請するとともに，新たな鍵ペアを生成し，コードサイニング証明書の発行申請及び受領を行った。鍵ペア生成時，Nサービスが一時停止しており，鍵ペアの保存に代替手段が必要になった。FIPS 140-2 Security Level 3の認証を受けたハードウェアセキュリティモジュール（HSM）は，⑨コード署名を付与する際にセキュリティ上の利点があるので，それを利用することにした。さらに，二つの対応とは別に，リポジトリの認証用SSH鍵を無効化した。

その後，開発部と協力しながら，P社内のPCでソースコードをコンパイルし，生成されたバイナリコードに新たなコード署名を付与した。JストアへのPアプリのアップロード履歴を確認したが，異常はなかった。新規の認証用APIキーを取得し，署名済みのバイナリコードをJストアにアップロードするとともに，⑩Kさんの二つの対応によってPアプリ利用者に生じているかもしれない影響，及びそれを解消するためにPアプリ利用者がとるべき対応について告知した。さらに，外部委託先であるN社に起因するインシデントとして関係当局に報告した。

設問1　本文中の下線①について，該当するものはどれか。解答群の中から全て選び，記号で答えよ。

解答群

ア　CIデーモンのプロセスを中断させる。

イ　いずれかのバックエンド上の全プロセスを列挙して攻撃者に送信する。

ウ　インターネット上のWebサーバに不正アクセスを試みる。

エ　攻撃者サイトから命令を取得し，得られた命令を実行する。

オ　ほかのNサービス利用者のビルドスクリプトの出力を取得する。

設問２　〔N 社のインシデントの発生と対応〕について答えよ。

(1)　本文中の下線②について，攻撃者による不正ログインの方法を，50 字以内で具体的に答えよ。

(2)　本文中の下線③について，RFC 9162 で規定されている技術を，解答群の中から選び，記号で答えよ。

解答群

ア　Certificate Transparency　　イ　HTTP Public Key Pinning

ウ　HTTP Strict Transport Security　　エ　Registration Authority

(3)　本文中の下線④について，このような手法の名称を，解答群の中から選び，記号で答えよ。

解答群

ア　DNS スプーフィング　　イ　ドメインフロンティング

ウ　ドメイン名ハイジャック　　エ　ランダムサブドメイン攻撃

(4)　本文中の下線⑤について，プロセス Y がシークレットを取得するのに使った方法として考えられるものを，35 字以内で答えよ。

(5)　図 2 中の下線⑥について，仮に，利用者が偽サイトでログインを試みてしまっても，攻撃者は不正ログインできない。不正ログインを防ぐ WebAuthn の仕組みを，40 字以内で答えよ。

(6)　図2中の［　a　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　CAA　　イ　CNAME　　ウ　DNSKEY　　エ　NS　　オ　SOA　　カ　TXT

設問３　〔N 社の顧客での対応〕について答えよ。

(1)　本文中の下線⑦について，K さんが開始した対応を踏まえ，予想される攻撃を，40 字以内で答えよ。

(2)　本文中の下線⑧について，必要な対応を，20 字以内で答えよ。

(3)　本文中の下線⑨について，コード署名を付与する際に HSM を使うことによって得られるセキュリティ上の利点を，20 字以内で答えよ。

(4)　本文中の下線⑩について，影響と対応を，それぞれ 20 字以内で答えよ。